# Popularizace vědy ve volnočasových aktivitách žáků SŠ - matematika

Modul je zaměřen na následující témata v kontextu věkové skupiny žáků středních škol: motivace k zájmu o studium technických a přírodovědných oborů, možnosti a typy popularizace vědy, získávání informací z nejnovějších vědeckých výzkumů, náměty pro aktivity zájmového kroužku, náměty projektů, experimentů, tipy na exkurze apod.

## Obsah:

- Motivace studentů ke studiu matematiky
- Možnosti a typy popularizace matematiky
- Nejnovější výzkumy
- Náměty aktivit pro popularizaci matematiky

Tento material vznikl z finanční podpory Evropského sociálního fondu a státního rozpočtu České republiky v rámci projektu „Popularizace vědy a badatelsky orientované výuky“, registrační číslo CZ.1.07/2.3.00/45.0007.

# Popularizace vědy ve volnočasových aktivitách žáků SŠ - matematika

Tento modul/kurz je zaměřen na následující témata v kontextu věkové skupiny žáků středních škol: motivace k zájmu o studium technických a přírodovědných oborů, možnosti a typy popularizace vědy, získávání informací z nejnovějších vědeckých výzkumů, náměty pro aktivity zájmového kroužku, náměty projektů, experimentů, tipy na exkurze apod.

**Autoři:**

**doc. RNDr. Jaroslav Hora, CSc.**
**Mgr. Lukáš Honzík, Ph.D.**
**Mgr. Martina Kašparová, Ph.D.**
**RNDr. Václav Kohout**



**K plnohodnotnému využití této studijní opory je nutný přístup k on-line zdrojům a materiálům.**

Tento materiál vznikl z finanční podpory Evropského sociálního fondu a státního rozpočtu České republiky v rámci projektu „Popularizace vědy a badatelsky orientované výuky“, reg .č. CZ.1.07/2.3.00/45.0007.

# 1 Popularizace matematiky - úvodem

Matematika dnes není, jak by se mohlo na první pohled mylně zdát, jen nudnou vědou o číslech, počítání a řešení rovnic. Naopak poskytuje základy pro řešení problémů v řadě dalších oborů, jako jsou například informatika a výpočetní technika, fyzika, strojírenství, ale také biologie, zeměpis, demografie, předpovídání počasí či predikování různých jiných jevů. Solidní znalost základů matematiky je v těchto oblastech nezbytná.

## 1.1 Motivace k zájmu o studium matematiky

Motivace k zájmu o studium matematiky se může ubírat mnoha směry. Zkusme přiblížit některé z nich a ukažme jejich prostřednictvím, proč je toto studium tak důležité.

V posledních desetiletích velmi vzrostla potřeba kódování a šifrování dat. V případě kódování jde o způsob, jímž jsou přenášená data upravována pro přenosové médium tak, aby byl přenos co nejefektivnější. Existují způsoby kódování, které častěji se vyskytujícím řetězcům znaků přiřazují relativně krátkou sekvenci, čímž dochází k zefektivnění přenosu nebo využití místa v datovém úložišti. Na druhou stranu šifrování je užíváno, pokud nechceme, aby někdo cizí "odposlouchával" nebo četl naši soukromou komunikaci nebo nahlížel do našeho bankovnictví. Proto byly vyvinuty různé druhy kódování a šifrování, přičemž obě tyto věci úzce souvisí s matematikou a jsou založeny na tzv. teorii čísel.

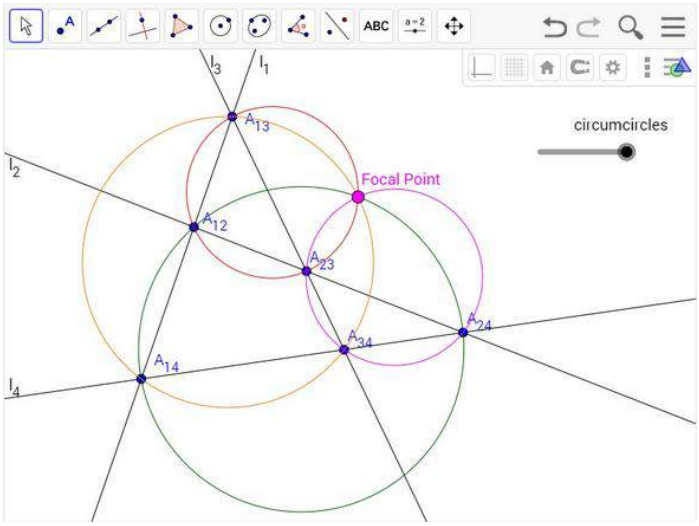
V obecnější rovině můžeme mluvit o vztahu matematiky a výpočetní techniky, který je oboustranně prospěšný. Na jedné straně matematika dodává potřebné znalosti, operace a početní prostředky, na nichž staví výpočetní technika (můžeme to říci i tak, že bez matematiky by prostě počítače nefungovaly), na druhé straně některé matematické úlohy jsou tak náročné a tedy "lidskými" způsoby neřešitelné, takže k jejich vyřešení je nutné využít výpočetní techniku.

Příkladem takového využití výpočetní techniky k řešení složitých matematických úloh může být kupříkladu předpovídání počasí, kdy jsou na základě aktuálních vstupních údajů a databáze obsahující data o vývoji počasí v minulosti počítány předpovědní modely.

### 1.2 Možnosti a typy popularizace matematiky

Matematika má na základních a středních školách dosti specifickou pozici - mezi žáky a studenty, pomineme-li výběrové třídy, nebývá moc oblíbená, protože ve školních lavicích se často setkávají s nepříliš živým a zajímavým výkladem a spoustou vzorečků. I přes tento "hendikep" je možné najít vhodné a pěkné způsoby, jak matematiku popularizovat.

Kromě již zmíněných věcí týkajících se spojení matematiky s výpočetní technikou nebo predikcí různých jevů (kdy přirozeně vyvstává otázka, jak to ten počítač vlastně dělá), se dají v dnešní době využít mnohé zajímavé matematické nástroje, které ulehčují pochopení daných matematických problémů. Mezi ty známější patří programy dynamické geometrie, jejichž prvním světově známým zástupcem byla Cabri Geometry firmy Cabrilog. Později na tyto základy navázaly programy GeoGebra, Cinderella, GEONExT a další. Programy mají jednoduché ovládání a zvládají toho leckdy i více než jen onu zmíněnou dynamickou geometrii.




*Ukázka programu GeoGebra (zdroj: https://www.geogebra.org/)*

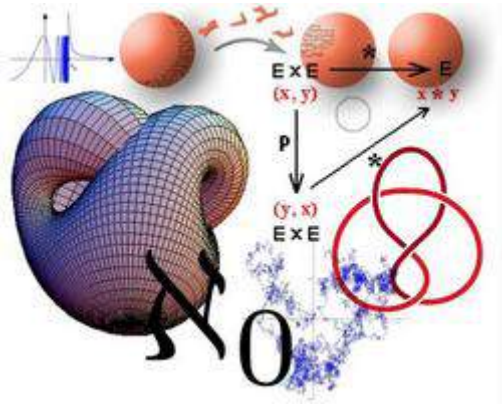
Obdobně lze mluvit i o programech výpočetních nabízejících uživatelům širokou škálu výpočetních prostředků, přičemž v případě webového prostředí Wolfram|Alpha (dostupný na stránce www.wolframalpha.com) se jedná nejen o výpočetní, ale též o databázový prostředek. Ukázka práce s některým ze zmíněných programů a jejich efektivní využití pro řešení matematického problému mohou být silným motivačním momentem.

Samostatnou kapitolou v popularizaci matematiky je oblast tzv. matematiky rekreační. Jedná se především o nejrůznější matematické hry a rébusy sloužící k procvičení mozkových závitů ve volných chvílích. Takovým asi nejznámějším rébusem je celosvětově známé sudoku, které i přes svůj orientální (japonský) název má částečně své kořeny i ve Francii 19. století. Existují však i další více či méně podobné rébusy, mezi nimiž můžeme jmenovat kakuro, nurikabe nebo fillomino.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 3 | | | | | 5 |
| | | 8 | 3 | 10 | | | 5 | |
| | 3 | | | | 4 | 4 | | |
| 1 | 3 | | 3 | | | 2 | | |
| | 2 | | | 3 | | | 2 | |
| | | 2 | | | 3 | | 1 | 3 |
| | | 4 | 4 | | | | 3 | |
| | 4 | | | 4 | 3 | 3 | | |
| 6 | | | | | 1 | | | |

*Ukázka zadání fillomina (zdroj: © 2005 Adam R. Wood, licencováno jako GFDL)*

### 1.3 Možnosti získávání informací z nejnovějších vědeckých výzkumů




V současné době nelze říci, že by se přímo v matematice samotné objevovaly nové poznatky. Toto období vývoje matematiky již spadá do historie nejpozději 19. století. V obecné rovině však dochází k vývoji a získávání nových poznatků v oblastech s matematikou úzce spojených, především v jejím různém aplikování (právě již zmíněné kódování a šifrování, vývoj nových algoritmů a postupů ap.). Z toho též vyplývá, že takto získané výsledky se kromě matematických časopisů (na českém trhu například časopisy*Matematika-fyzika-informatika* - časopis je dostupný v elektronické verzi zde, *Učitel matematiky* atd.) vyskytují v širokém spektru časopisů věnovaných dalším oborům.

---

Zdroj obrázku: commons.wikimedia.org, volné dílo

# 2 Náměty pro aktivity zájmového kroužku

## 2.1 Náměty aktivit pro popularizaci matematiky

### Řešení jednoduchých optimalizačních úloh pomocí softwaru dynamické geometrie

Jednoduché optimalizační úlohy zadávané většinou jako úlohy slovní lze dosti často vhodně řešit použitím grafické metody, resp. tuto metodu využít ke zjednodušení komplikovaného početního řešení. Oproti klasickému "statickému" znázornění náčrtkem na papíře lze úspěšně postavit některé nástroje dynamické geometrie, především aplikaci GeoGebra (pro nekomerční užití zdarma dostupná na stránce http://www.geogebra.org), v níž uživatel může nejen konstruovat geometrické objekty, pracovat s geometrickými zobrazeními či například vyšetřovat průběhy funkcí, ale využívat ji i způsoby, které u dalších programů dynamické geometrie nejsou možné. V případě řešení jednoduchých optimalizačních úloh je tak možné vytvořit názorný interaktivní náčrt zadané situace a zkoumat změny, které nastanou při změně vstupních parametrů.

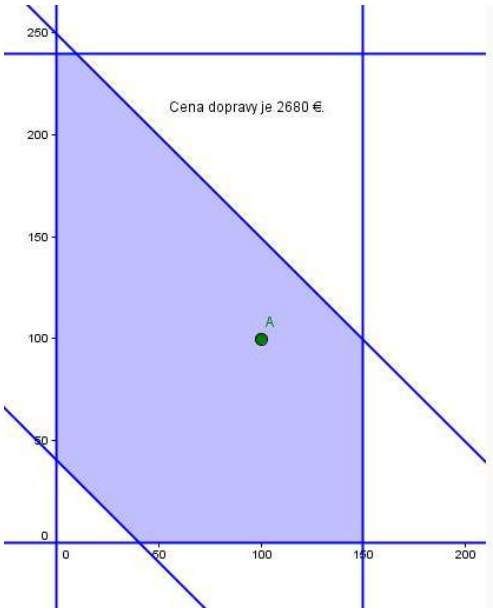
**Příklad** (Rozvoz mléka)**:** Mléko z mlékárenských závodů ve městech A a B se vozí také do měst R, S a T. Denně se může z A dodat 250 přepravek s mlékem a z B 350. Denně je potřeba dodat 150 přepravek do R, 240 přepravek do S a 210 přepravek do T. Nalezněte způsob rozvozu, při kterém budou náklady nejnižší. Náklady na přepravu jedné přepravky z mlékárenského závodu do místa prodeje jsou v tabulce.

| cena v € | R | S | T |
|---|---|---|---|
| A | 4 | 3 | 5 |
| B | 5 | 6 | 4 |

**Řešení:** Hledání optimalizovaného výstupu v zásadě odpovídá nalezení extrému (minima) funkce více proměnných v oblasti omezené danými podmínkami. V našem případě je nejprve nutné volit dvě neznámé $x$ a $y$ udávající počty přepravek dopravených z A do R a z B do R a počty zbývajících přepravek vyjádřit podle podmínek uvedených v zadání.

| počty přepravek | R | S | T |
|---|---|---|---|
| A | $x$ | $y$ | $250 - x - y$ |
| B | $150 - x$ | $240 - y$ | $x + y - 40$ |

Z obou tabulek je následně možné konstruovat tzv. účelovou funkci, která vypovídá o výstupní hodnotě nákladů na přepravu $f(x, y) = 4x + 3y + 5\cdot(250 - x - y) + 5\cdot(150 - x) + 6\cdot(240 - y) + 4\cdot(x + y - 40)$, po úpravě $f(x, y) = -2x - 4y + 3280$. Podmínky pro omezení oblasti pak také vychází z vyjádření v tabulce: $x \geq 0$, $x \leq 150$, $y \geq 0$, $y \leq 240$, $x + y \leq 250$, $x + y \geq 40$. Zanesené do soustavy souřadnic v programu GeoGebra jsou vidět na obrázku, kde tvoří $n$-úhelník.




*Grafické znázornění podmínek (obrázek vlastní tvorby)*

Na tento *n*-úhelník lze v programu umístit bod, třeba bod *A*, a též textové pole, do něhož bude vypisována funkční hodnota účelové funkce pro příslušné souřadnice *x* a *y* bodu *A*. Změnou polohy bodu *A* je dosaženo změny funkční hodnoty a jeho posunováním ve vymezené oblasti je možné experimentálně odhalit, kde nabyde funkce *f*(*x*, *y*) své minimum. Interaktivní figura odpovídající zadání příkladu je k nalezení v sekci Multimédia k badatelské aktivitě.

Hodnoty souřadnic *x* a *y* bodu *A* pak budou částí hledaného řešení zadané úlohy. V našem případě nalezneme minimum účelové funkce ve vrcholu *n*-úhelníku o souřadnicích [10; 240], následně je možné dopočítat i zbývající neznámé.

Tabulka s optimalizovaným rozpisem rozvozu přepravek vypadá následovně:

| počty přepravek | R | S | T |
|---|---|---|---|
| A | 10 | 240 | 0 |
| B | 140 | 0 | 210 |

a slovní odpověď zní, že nejnižší náklady na přepravu budou tehdy, pokud bude z A do R přepraveno 10 přepravek, z A do S 240, z B do R 140 a z B do T 210 přepravek.

Obdobnými způsoby lze samozřejmě řešit i další jednoduché optimalizační úlohy, pro ilustraci uvádíme některá další zadání podobných příkladů:

**Příklad** (Tovární hala)**:** V tovární hale je instalováno 60 strojů typu I a 40 strojů typu II, podnik však může získat na práci ve druhé směně nejvýše 80 dělníků. Na každém stroji typu I vyrobí dělník za směnu nejvýše 200 kusů výrobku A, na každém stroji typu II nejvýše 300 kusů výrobku B. Plán požaduje vyrobit aspoň 12.000 kusů celkem za směnu. Každý stroj I má hodinový příkon 5 kW, každý stroj II má hodinový příkon 15 kW, pro celou halu je limit

750 kW. Při kterém rozdělení dělníků ke strojům typu I a II dosáhne druhá směna maximálního čistého zisku pro podnik, jestliže z jednoho kusu výrobku A je zisk 80 euro a z jednoho kusu výrobku B je zisk 100 euro?

**Příklad** (Osevní plocha)**:** Na celkové výměře maximálně 10 hektarů se má pěstovat pšenice a cukrovka tak, aby tržní produkce byla co největší. Pšenice se z agrotechnických důvodů nesmí pěstovat na více než 4 hektarech. Jako činitele výroby uvažujeme jen počet pracovních hodin, přičemž zdrojem výroby je celkový počet pracovních hodin v jednotlivých měsících špičkových prací, které jsou uvedeny v tabulce.

| potřeba pracovních hodin na 1 hektar | pšenice | cukrovka | možný počet pracovních hodin |
|---|---|---|---|
| v květnu | 1 | 5 | 18 |
| v červnu | 0 | 1 | 5 |
| v červenci | 5 | 2 | 21 |
| tržní produkce z 1 ha v tisících euro | 4 | 6 | |

**Příklad** (Krmná směs)**:** Z krmných surovin A a B je třeba namíchat nějaké množství krmné směsi tak, aby byly splněny tři živinové požadavky P, Q a R a aby směs byla co nejlevnější. Údaje potřebné k výpočtu jsou v tabulce.

| obsah živin P, Q, R v 1 kg suroviny A, B | P | Q | R | cena 1 kg suroviny |
|---|---|---|---|---|
| A | 50 g | 60 g | 250 g | 15 euro |
| B | 75 g | 200 g | 100 g | 10 euro |
| požadavek na obsah živin | 900 g | 1200 g | 2000 g | |

**Příklad** (Fotoaparáty)**:** Závod na výrobu fotoaparátů vyrábí dva druhy A a B. Velkoobchodní cena aparátu A je 1000 euro, fotoaparátu B 500 euro. Jestliže odečteme od těchto cen vlastní náklady spojené s výrobou každého kusu fotoaparátu (pro A je to 600 euro, pro B 200 euro), můžeme říci, že čistý zisk podniku za jeden fotoaparát A je 400 euro, za fotoaparát B 300 euro. Kapacitu dílen vyjádřenou v počtu kusů výrobků A a B zhotovených za kvartál vyjadřuje tabulka. Je třeba zjistit, kolik fotoaparátů A a kolik fotoaparátů B za kvartál má závod vyrobit, aby byl zisk maximální. (Předpokládáme, že závod není při výrobě fotoaparátů vázán žádným plánem, pokud jde o počet kusů jednotlivých typů výrobků.)

| číslo dílny | výrobní náplň | kapacita dílny za kvartál při výrobě fotoaparátu A | kapacita dílny za kvartál při výrobě fotoaparátu B |
|---|---|---|---|
| 1 | výroba součástek pro typ A | 100 | - |
| 2 | výroba součástek pro typ B | - | 200 |
| 3 | montáž mechanických dílců | 100 | 150 |
| 4 | montáž jemné optiky | 100 | 200 |
| 5 | konečná montáž | 150 | 100 |
| 6 | zkušebna | 200 | 200 |

**Metodický list pro badatelskou aktivitu**

| | | |
|---|---|---|
| Téma | Grafické řešení jednoduchých optimalizačních úloh | |
| Tematický celek | Slovní úlohy | |
| Motivační rámec aktivity | Plánování například firemní výroby nebo rozvozu výrobků je jedním z důležitých obvětví obchodu. Žáci se při řešení jednoduchých optimalizačních úloh dostávají do role těchto manažerů optimalizátorů odpovědných za zvýšení zisku či naopak za snížení nákladů. | |
| Počet žáků | 10-15 | |
| Věk žáků | 13+ | |
| Pomůcky | Počítač, příslušné softwarové vybavení | |
| Stručný popis aktivity s využitím přístroje | Experimentální hledání řešení jednoduchých optimalizačních úloh pomocí programu dynamické geometrie GeoGebra | |
| Vhodné místo | Počítačová učebna | |
| Cíle aktivity | Žáci budou schopni zvládnout jednoduché úkony týkající se práce s programem GeoGebra (potažmo i s jinými programy dynamické geometrie), pochopit souvislost mezi vstupními parametry a měnící se hodnotou výstupu, nalézt alespoň přibližně správné vstupní hodnoty pro daný hledaný výstup, řešit jednoduché optimalizační úlohy. | |
| Rozvíjené kompetence | Kompetence k řešení problémů, komunikativní, pracovní,... | |
| Předchozí znalosti | Aktivita navazuje na řešení slovních úloh, práci s funkcemi a geometrickými objekty. | |
| Mezipředmětové vztahy | Informatika, Člověk a svět | |
| Časový plán | Fáze činnosti s | Metody a formy, motivace |

| | | |
|---|---|---|
| | přístrojem | |
| 0-15 | - | frontální: nastínění situace - nutnost nalezení optimálního způsobu rozvozu mléka, aby se ušetřilo<br>skupinová: hledání vhodného způsobu zápisu a vyjádření zadaných informací |
| 15-25 | grafické vyjádření zadaných podmínek a dalších informací | frontální: grafické zpracování zadání úlohy v počítači, interpretace podmínek, zavedení bodu, s nímž se bude experimetovat |
| 25-30 | nalezení extrému a řešení | frontální s dialogem: nalezení extrému, interpretace zjištěných skutečností, sestrojení závěru |
| 30-45 | samostatná práce s programem | individuální či skupinová (v malých skupinách, ve dvojicích): experimetování žáků s dalším zadaným příkladem jednoduché optimalizace |
| Hodnocení | Hodnocení neprováděno, případně prováděno jen okrajově v závislosti na zapojení do diskuze o hledaném řešení a na základě zvládnutí práce s programem dynamické geometrie. | |
| Návaznosti | Další práce s programem dynamické geometrie, například grafické řešení slovních úloh o pohybu. | |

**Multimédia k badatelské aktivitě**

Interaktivní geometrická figura k příkladu jednoduché optimalizační úlohy je ke stažení zde. K jejímu spuštění je nutné mít nainstalovanou a aktualizovanou Javu a program GeoGebra.

*Vyznačená modrá oblast (n-úhelník) je oblastí roviny omezenou podmínkami vycházejícími ze zadání slovní úlohy. Bodem A, který je k n-úhelníku přichycen, lze pohybovat a v závislosti na jeho poloze (a tedy změně jeho souřadnic v rovině) se mění hodnota účelové funkce odpovídající ceně. Posunutím bodu do některého z vrcholů n-úhelníku lze objevit minimum (nebo také maximum) účelové funkce, a tedy i optimální rozdělení převážených přepravek.*

**Izoperimetrické úlohy (do 45 min)**

Několika pokusy provedenými fyzicky i výpočtem jsou studenti motivováni k seznámení se s typem úloh, v nichž se požaduje nalezení hodnot či křivek poskytující maximální či minimální hodnotu funkce při zadaných podmínkách. Izoperimetrické úlohy jsou základním typem úloh variačního počtu. Variační počet má široké uplatnění ve fyzice zejména s ohledem na názor, že fyzikální děje probíhají tak, že splňují nějakou extremální úlohu. (Např. nejkratší dráha světelného paprsku při průchodu různými prostředími, úloha o brachystochroně - o nalezení dráhy hmotného bodu spojující dva body ve svislé rovině tak, aby se hmotný bod z výchozího do koncového bodu pohyboval pouze vlivem gravitace a zvládl to za nejkratší možný čas atd.).

**Úkol 1.** Pomocí řetízku nebo snadno ohybatelného drátu vymodeluj pět různých trojúhelníků na čtvercové síti. Užitím čtvercové sítě urči přibližně jejich obsah.

Který z trojúhelníků má největší obsah? Porovnej své výsledky s ostatními a charakterizuj trojúhelník s největším obsahem, kterého bylo ve skupině dosaženo.
-> Čím se trojúhelník více blíží rovnostrannému trojúhelníku, tím má větší obsah.

Který z trojúhelníků má největší obvod?
-> Všechny trojúhelníky mají stejný obvod daný rozměrem drátu nebo řetízku.

Má tedy smysl uvažovat o rovinných útvarech, které mají při daném obvodu největší obsah. To je základ tzv. izoperimetrických úloh.

**Izoperimetrická úloha**
Slovo „izoperimetrický“ vzniklo složením ze slov „isos“ a „perimetreo“. Slovo „isos“ pochází z řečtiny a v překladu znamená „stejný“. Na základě svých znalostí angličtiny (perimeter - obvod) snadno uhádneš význam druhého slova řeckého původu. Izoperimetrické úlohy se v užším smyslu zabývají útvary se stejným obvodem.

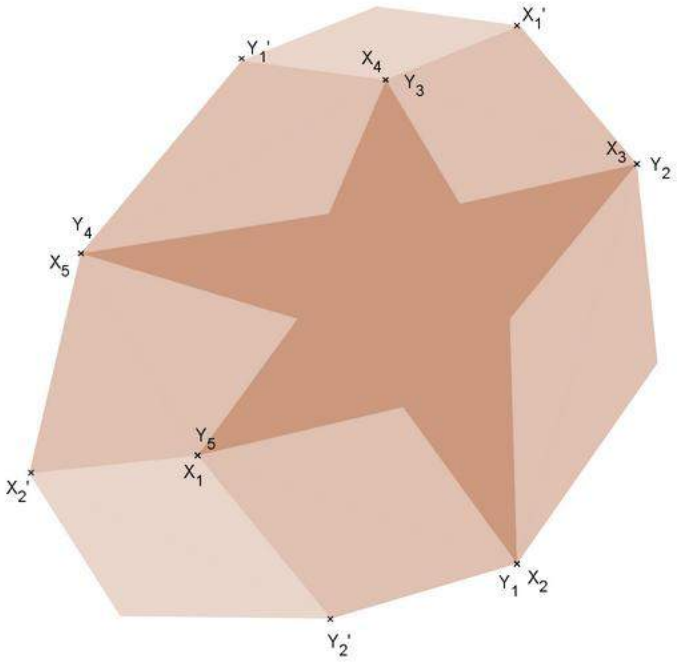
**Úkol 2.** Dokážeš odhalit, který z pravoúhelníků se stejným obvodem má největší obsah? Můžeš opět využít řetízek nebo drátek a čtvercovou síť.
-> Při daném obvodu má největší obsah ze všech pravoúhelníků čtverec.

***O moudrosti včel***
Pappos Alexandrijský napsal někdy ve 4. stol. n. l. ve své práci *Synagogé* v 5. knize nazvané *O moudrosti včel*:
Včely znají skutečnost, která je pro ně užitečná, a to, že šestiúhelník je větší než čtverec a trojúhelník a že se do něj vejde více medu při stejném výdeji materiálu na postavení plástve.

**Úkol 3.** Odhadni, který rovinný útvar má při daném obvodu maximální obsah. Nápověda: Zvyšuj počet stran konvexních mnohoúhelníků vytvářených z řetízku nebo drátu.
-> Intuitivně tušíme to, co napsal již Pappos, že ze všech rovinných útvarů se stejným obvodem je větší vždy ten, který má větší počet úhlů, a největší z nich je kruh jako případ "nekonečněúhelníku".

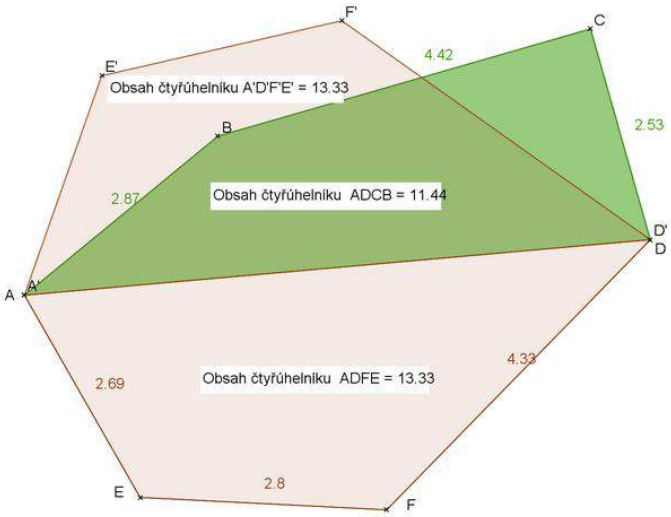
**Proč má kruh největší obsah při daném obvodu?** (Důkaz proveden podle [1].)
(a) Předně rovinný útvar daného obvodu a maximálního obsahu musí být konvexní. Pokud by rovinný útvar nebyl konvexní, lze na něm vhodně zvolit dvojice bodů $X_1$, $Y_1$, $X_2$, $Y_2$, ... tak, že všechny vnitřní body úseček $X_1Y_1$, $X_2Y_2$, ... nenáleží útvaru. Zobrazíme-li oblasti

mezi úsečkami $X_1Y_1$, $X_2Y_2$, ... a hranicí nekonvexního útvaru v osové souměrnosti s úsečkami $X_1Y_1$, $X_2Y_2$, ..., dostaneme útvar, který má stejný obvod, ale větší obsah, viz obrázek.




Obr. 1 - vytvořen pomocí programu GeoGebra, Zdroj: vlastní tvorba

(b) Rozdělují-li dva body A, D obvod útvaru na polovinu, pak v rovinném útvaru daného obvodu a maximálního obsahu úsečka AD dělí útvar na dva útvary stejného obsahu. Pokud by rovinný útvar popsanou vlastnost neměl, pak by bylo možno v osové souměrnosti s osou AD zobrazit část útvaru s větším obsahem do poloroviny s částí útvaru menšího obsahu, viz obrázek. Na obrázku je šestiúhelník ABCDFE rozdělen na čtyřúhelníky ADCB a ADFE se stejnými obvody, ale různými obsahy. Šestiúhelník AEFDF'E' má zjevně větší obsah, neboť čtyřúhelník A'D'F'E', který je obrazem čtyřúhelníku AEFD v osové souměrnosti s osou AD, má větší obsah než čtyřúhelník ADCB.




Obr. 2 - vytvořen pomocí programu GeoGebra, Zdroj: vlastní tvorba

(c) Zbývá ukázat, že ze všech křivek dané délky a s koncovými body A, D na pevně dané přímce uzavírá s úsečkou AD největší plochu půlkružnice. Důkaz lze najít např. v [1].

**Úkol 4.** Který rovinný útvar s daným obsahem má nejmenší obvod?
-> Je to opět kruh.
Pokud by to nebyl kruh K, ale nějaký útvar U, pak by pro jejich obsahy platilo $S_K = S_U$ a pro jejich obvody $o_K > o_U$. Vezměme kruh K', který má obvod $o_U$. Kruh s menším obvodem má menší obsah, proto $S_{K'} < S_K = S_U$. Na druhou stranu při daném obvodu $o_U$ má největší obsah kruh, tedy $S_{K'} > S_U = S_K$. To vede ke sporu a k tomu, že předpoklad existence útvaru U se stejným obsahem, jako má kruh K, a obvodem menším, než je obvod kruhu, nebyl správný.
Pokud bychom naopak věděli, že rovinným útvarem s daným obsahem a nejmenším možným obvodem je kruh, pak by šlo ukázat, že při daném obvodu má kruh největší obsah. Opět, pokud by při daném obvodu neměl největší obsah kruhu K, ale nějaký útvar U, pak by pro jejich obvody platilo $o_K = o_U$ a pro jejich obsahy $S_K < S_U$. Vezměme kruh K', který má obsah$S_U$, tj. $S_{K'} = S_U$. Kruh s větším obsahem má větší i obvod, proto $o_{K'} > o_K = o_U$. Na druhou stranu při daném obsahu $S_U$ má nejmenší obvod kruh, tedy $o_{K'} < o_U = o_K$, což vede ke sporu a nekonstruktivnímu potvrzení neexistence daného útvaru U.

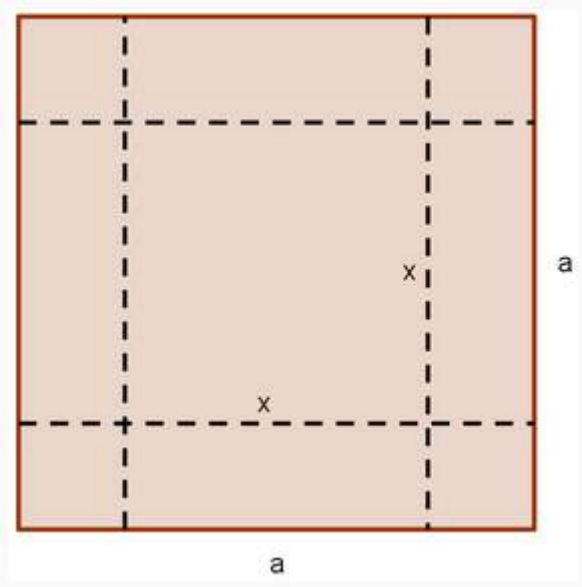
**Ekvivalentnost dvou tvrzení o kruhu**
Ukázali jsme, že tvrzení o tom, že kruh je rovinný útvar, který má při daném obvodu největší obsah, je ekvivalentní s tvrzením, že kruh je rovinný útvar, který má při daném obsahu nejmenší obvod.

**Úkol 5.** Vymysli analogickou úlohu k úkolu 3 v prostoru a její řešení.
-> Který prostorový útvar má při daném povrchu největší objem? Který prostorový útvar má při daném objemu nejmenší povrch?
K analogické úvaze očekáváme analogický útvar jako řešení, tím je v tomto případě koule.

Řešme nyní úlohy v prostoru, v nichž se za daných podmínek má najít maximální objem nebo minimální povrch.

**Úkol 6.** Ze čtvercového kousku pozinkovaného plechu o straně a = 15 cm se má vyrobit nádoba se čtvercovým dnem shora otevřená. Jaký největší objem může mít nádoba? (Zadání úlohy převzato z [3], str. 312.)
Zkus řešit úlohu experimentálně - tvoř různé nádoby s využitím čtverce vystřiženého ze čtverečkovaného papíru. Objemy takových nádob se snadno vypočtou.

-> Má-li mít nádoba čtvercové dno a maximální objem, musí být střed čtverce, který reprezentuje dno, shodný se středem čtverce - pozinkovaného plechu. Jinak by boční stěny ve tvaru obdélníku neměly stejné rozměry. Označme hledanou délku hrany podstavy x, potom podstavu tvoří čtverec s rozměrem x a boční stěny obdélníky s rozměry x a ½.(a-x).




Obr. 3 - vytvořen pomocí programu GeoGebra, Zdroj: vlastní tvorba

Pro objem nádoby se čtvercovou podstavou při daném označení platí:
$V = x^2.½.(a-x)$.
Úkolem je najít hodnotu x, pro niž je V maximální.
(1) Ti, kdož znají diferenciální počet, si s úlohou snadno poradí. Výpočet první derivace vede k jedinému smysluplnému stacionárnímu bodu $x = 2a/3$ a výpočtem druhé derivace se ověří, že jde skutečně o bod, v němž V dosahuje maximální hodnoty, a to $V = (2a/3)^2.½.(a-2a/3) = 2a^3/27$.
(2) Největší objem však lze najít i elementárním způsobem - řešením nerovnice s parametrem. Jako parametr volíme např. m - maximální hodnota objemu. Pak pro každé přípustné x platí:
$x^2.½.(a-x) \leq m$
Hledáme takovou hodnotu parametru m, aby předchozí rovnice měla řešení pro libovolné přípustné x. Vzhledem k technické náročnosti tohoto postupu, zvolíme postup popsaný v bodě (3).
(3) V tomto postupu využijeme nerovnost mezi aritmetickým a geometrickým průměrem (AG-nerovnost),

$$\sqrt[n]{a_1.a_2 \dots a_n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n}$$

pro n = 3, tj. ve tvaru

$$\sqrt[3]{a_1.a_2.a_3} \leq \frac{a_1 + a_2 + a_3}{3}$$

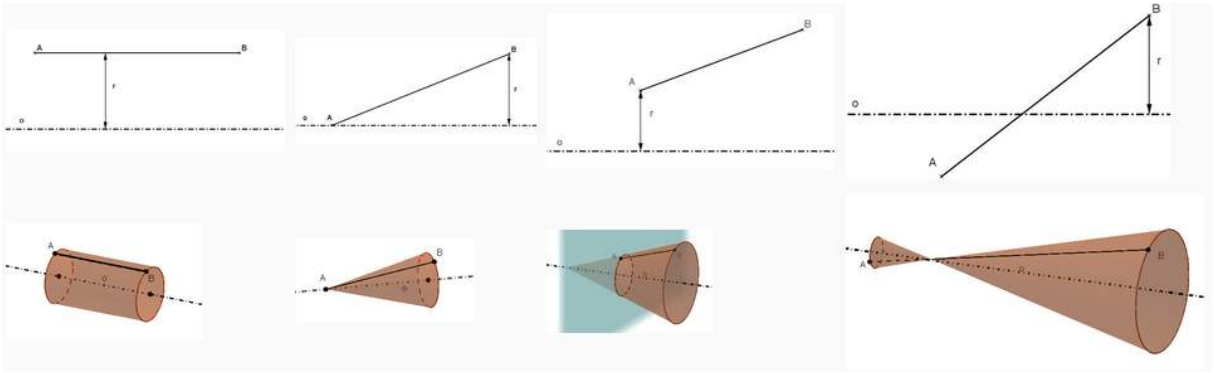
Funkci $V = x^2.½.(a-x)$ lze psát též ve tvaru $V = x.x.(½.a - ½.x)$. Její maximum nastane ve stejném bodě x, i když ji vynásobíme 4. (Čtyřmi násobíme z toho důvodu, aby se v součtu činitelů vyloučila neznámá x, viz níže.) Hledejme proto maximum funkce
$4V = x.x.(2a - 2x)$
Ta je pro využití AG-nerovnosti vhodnější než původní, protože součet činitelů v jejím předpisu je roven konstantě, $x + x + (2a - 2x) = 2a$. S využitím AG-nerovnosti pro n = 3 dostáváme

$$\sqrt[3]{x.x.(2a-2x)} \leq \frac{2a}{3}$$

a odtud je po umocnění na třetí
$4V = x.x.(2a - 2x) \leq (8/27)a^3$
$V = x.x.½.(a - x) \leq (2/27)a^3$

Maximální hodnota objemu je tedy $2a^3/27$. Této hodnoty objem dosáhne jen tehdy, když v AG-nerovnosti nastane rovnost. Výrazy na obou stranách AG-nerovnosti se rovnají, pokud $a_1 = a_2 = a_3$. V našem případě tedy x = x = 2a - 2x. Poslední vztah vede k hodnotě x = 2a/3. Pro a = 15 cm bude mít nádoba maximální objem, zvolíme-li její podstavnou hranu x = 10cm. Objem nádoby bude 250 $cm^3$.
(4) Ti, kteří dávají přednost řešení s využitím počítače, mohou přibližnou hodnotu maximálního objemu V i hodnotu x určit pomocí funkce "Řešitel" v aplikaci Microsoft Excel. Je-li k dispozici dokonce program Mathematica, můžeme využít vestavěných funkcí pro řešení postupem (1) nebo (2).

**Úkol 7.** Při jaké vzájemné poloze úsečky AB, |AB| = l, a osy o, kolem které úsečka rotuje, má vzniklé rotační těleso minimální obsah pláště za podmínky, že aspoň jeden bod úsečky je od osy o vzdálen právě r, l/2 < r < l?
-> Rozmysleme nejprve, jaká tělesa mohou vzniknout rotací úsečky AB kolem osy o.



Obr. 4 - vytvořeny pomocí programu GeoGebra, Zdroj: vlastní tvorba

**I.** Je-li úsečka AB rovnoběžná s osou o, kolem níž se otáčí, pak rotací vznikne plášť válce s poloměrem odpovídajícím vzdálenosti úsečky AB od osy a s výškou, která je rovna délce úsečky AB, viz obrázek. Plášť lze rozvinout do obdélníku s rozměry |AB| = l a o = 2πr, proto je obsah pláště

$S_{pl} = 2\pi rl.$

**II.** Je-li úsečka AB různoběžná s osou o tak, že s ní má společný jeden z krajních bodů, vznikne její rotací kolem osy o plášť kužele s kruhovou podstavou o poloměru r a s výškou $\sqrt{(l^2 - r^2)}$, viz obrázek. Plášť kužele tvoří kruhová výseč, která vznikla z kruhu o poloměru |AB| = l. Obsah pláště je roven

$S_{pl} = \pi rl.$

**III.** Pokud je AB opět různoběžná s osou o jako v případě II., ale nemá s osou žádný společný bod, vytvoří rotující úsečka plášť komolého kužele. Protože jeden z krajních bodů,

např. bod A, je od osy o vzdálen r, je krajní bod B od osy vzdálen ρ, kde buď ρ > r (viz obrázek), nebo ρ < r (bez obrázku). Obsah pláště komolého kužele s podstavami o poloměrech r a ρ můžeme vypočítat z předpisu

$S_{pl} = \pi(r + \rho)l.$

**IV.** Úsečka AB může být s osou o různoběžná také tak, že s ní má společný jeden bod. V takovém případě vzniknou dva pláště kuželů $K_1$, $K_2$ se společným vrcholem, tj. plášť dvojkužele. Vzhledem k podmínce, že aspoň jeden bod úsečky je od osy o vzdálen aspoň r, má jeden z kuželů, např. $K_2$, poloměr r. Rozměry $K_1$ určíme v závislosti na délce strany kužele $K_2$, kterou označme x. Délka strany $K_1$ je l-x. Kužely jsou podobné s koeficientem podobnosti daným poměrem jejich stran, tj. (l-x):x. Proto je poloměr $K_1$ roven r.(l-x):x. Obsah pláště, který vznikne rotací úsečky různoběžné s osou, která s ní má jeden společný bod, je dán předpisem

$S_{pl} = \pi rx + \pi r(l-x).(l-x):x,$

což lze upravit na tvar

$S_{pl} = \pi r[2x - 2l + l^2/x].$

• Z vyvozených vztahů je zřejmé uspořádání prvních tří těles podle obsahu pláště: válec, komolý kužel, kužel pro ρ < r, resp. komolý kužel, válec, kužel pro ρ > r, kde ρ je vzdálenost bodu B od osy. Zda je plášť dvojkužele pro nějaké vhodné x menší než plášť kužele a pro jaké x to případně nastane, zjistíme výpočtem.

• Zapišme podmínku, že obsah pláště dvojkužele je menší než obsah pláště kužele, nerovnicí:

$\pi r[2x - 2l + l^2/x] < \pi rl$

Jednoduchými úpravami dospějeme k nerovnici

$2x^2 - 3lx + l^2 < 0,$

kterou lze napsat v součinovém tvaru:

$(2x - l)(x - l) < 0$

Řešením nerovnice jsou všechna x větší než l/2 a menší než l. Zvolíme-li stranu x kužele $K_2$ s poloměrem r v rozmezí od l/2 do l, bude obsah pláště dvojkužele menší než obsah pláště kužele. Pro x = l/2 a x = l dostaneme rovnost obsahů plášťů. Pro x = l je to evidentní, protože v takovém případě je dvojkužel pouze kuželem. Pro x = l/2 získáváme elementární poznatek, že obsah pláště kužele se stranou l je stejný jako součet obsahů plášťů dvou stejných kuželů s poloviční stranami a stejným poloměrem.

• Má tedy smysl zjistit, pro kterou hodnotu x je $S_{pl}$, obsah pláště dvojkužele, nejmenší. Opět se nabízí několik možností, jak zjistit minimum, v závislosti na znalostech a technických podmínkách.

**(1)** Užitím diferenciálního počtu. Po zderivování funkce $S_{pl}$ podle x lze stacionární bod určit z rovnice $\pi r[2 - l^2/x^2] = 0$. Obsah pláště je tedy nejmenší, když $x = l.\sqrt{2}/2$, tj. když vrchol dvojkužele rozdělí úsečku AB v poměru $1:\sqrt{2}$.

**(2)** Elementární postup vede k diskusi řešení nerovnice s parametrem $S_{pl} \geq m$, tj.

$\pi r[2x - 2l + l^2/x] \geq m,$

kde m je minimiální obsah pláště dvojkužele. Zjistíme z ní, pro které hodnoty parametru m má nerovnice za řešení libovolné x větší než l/2 a menší než l, což jsou všechna x, která nás zajímají. Předchozí nerovnici upravíme na kvadratickou nerovnici

$x^2 - x[l + m/(2\pi r)] + l^2/2 \geq 0,$

a následně doplněním na čtverec na nerovnici

$\{x - [l/2 + m/(4\pi r)]\}^2 + l^2/2 - [l/2 + m/(4\pi r)]^2 \geq 0.$

Ta je ve tvaru $X^2 + A \geq 0$, o kterém víme, že má za řešení libovolné X, když $A \geq 0$. Proto má předchozí nerovnice za řešení libovolné x pro

$l^2/2 - [l/2 + m/(4\pi r)]^2 \geq 0,$

tj. pro

$l^2/2 \geq [l/2 + m/(4\pi r)]^{2.}$

Protože l, m, π, r jsou kladná čísla, je uvedená nerovnice ekvivalentní s nerovnicí

$l/\sqrt{2} \geq l/2 + m/(4\pi r).$

Po jednoduchých úpravách je

$2\pi rl(\sqrt{2} - 1) \geq m,$

a tedy $S_{pl} = 2\pi rl(\sqrt{2} - 1)$ je nejmenší obsah pláště dvojkužele v souladu se zjištěním z bodu (1).

**(3)** Stejně jako v úkolu 6 lze i nyní pro nalezení extrému využít nerovnost mezi aritmetickým a geometrickým průměrem. Tentokrát využijeme AG-nerovnost pro n = 2 na součet $2x + l^2/x$, který se objevuje v předpisu pro výpočet obsahu pláště dvojkužele. Pro aritmetický průměr výrazů 2x a $l^2/x$ platí:

$[2x + l^2/x]/2 \geq \sqrt{[(2x).(l^2/x)]}.$

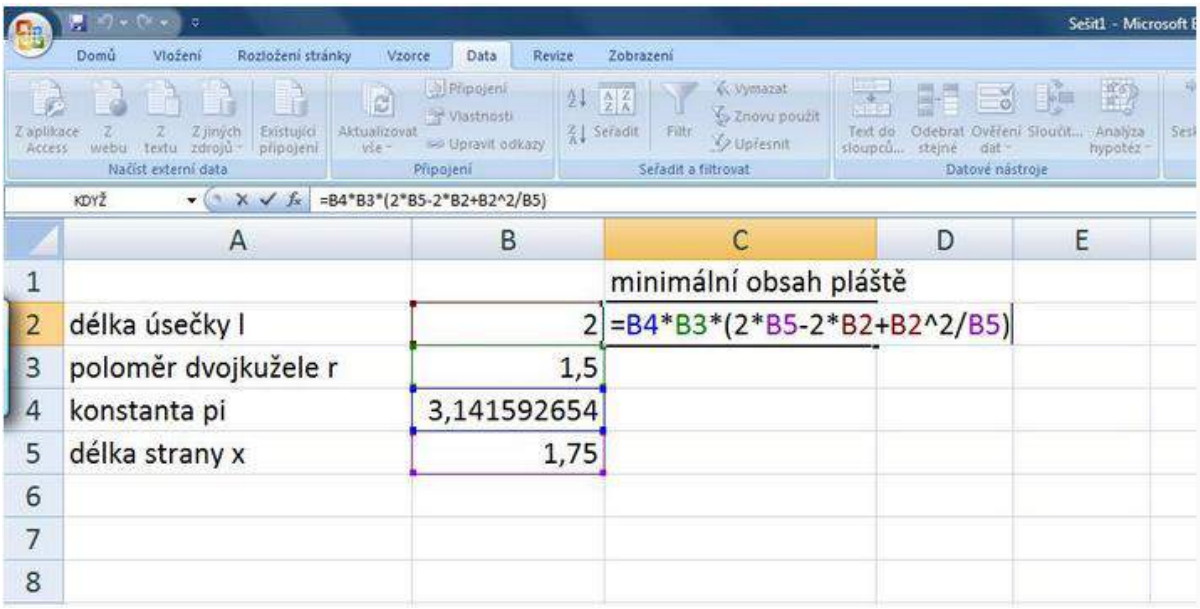
Obě strany nerovnosti vynásobíme 2, odečteme od nich 2l a výsledek vynásobíme πr. Tím dostaneme

$\pi r[2x - 2l + l^2/x] \geq \pi r.2l.(\sqrt{2} - 1),$

tedy podmínku pro nejmenší možný obsah pláště dvojkužele.

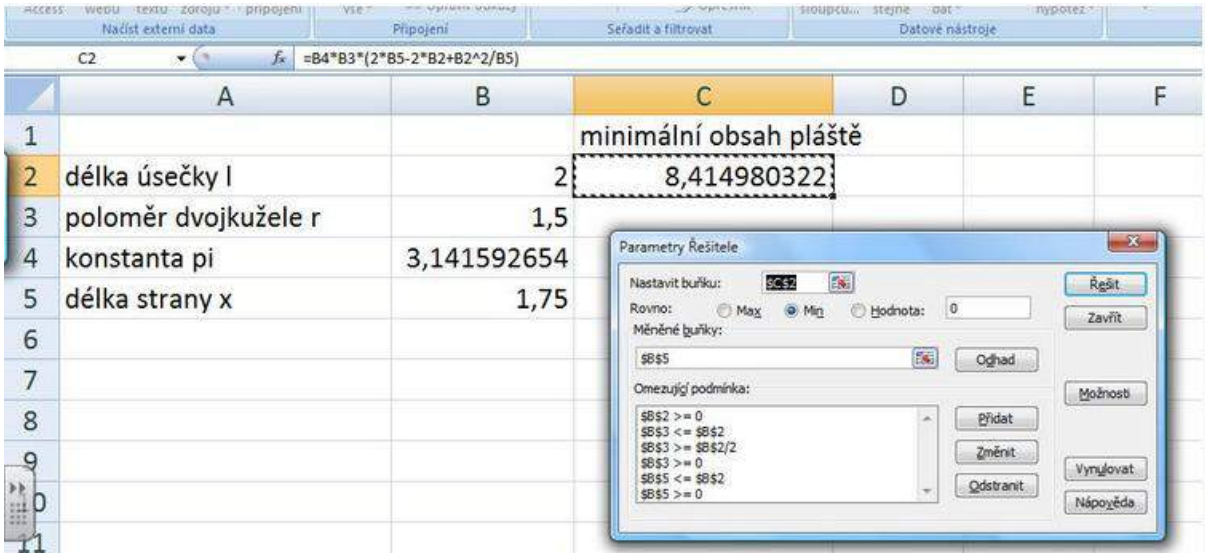
**(4)** Ukažme, jak by se minimum našlo pomocí funkcí dostupných v Excelu a v programu Mathematica.

A. Funkce "Řešitel" v Excelu umí najít hodnotu výrazu, která se rovná zadané hodnotě anebo je minimální či maximální, při změně některých členů zkoumaného výrazu. Zadejme v sešitě hodnoty tak, jak je vidět na obrázku. V buňce s minimálním obsahem pláště je zadán předpis pro výpočet obsahu pláště dvojkužele, který budeme minimalizovat. Délka strany AB byla stanovena pevně jako 2, poloměr r jako 1,5, délka strany x většího kužele jako 1,75, protože Excel umí počítat jen s konkrétními čísly, nikoli s proměnnými.



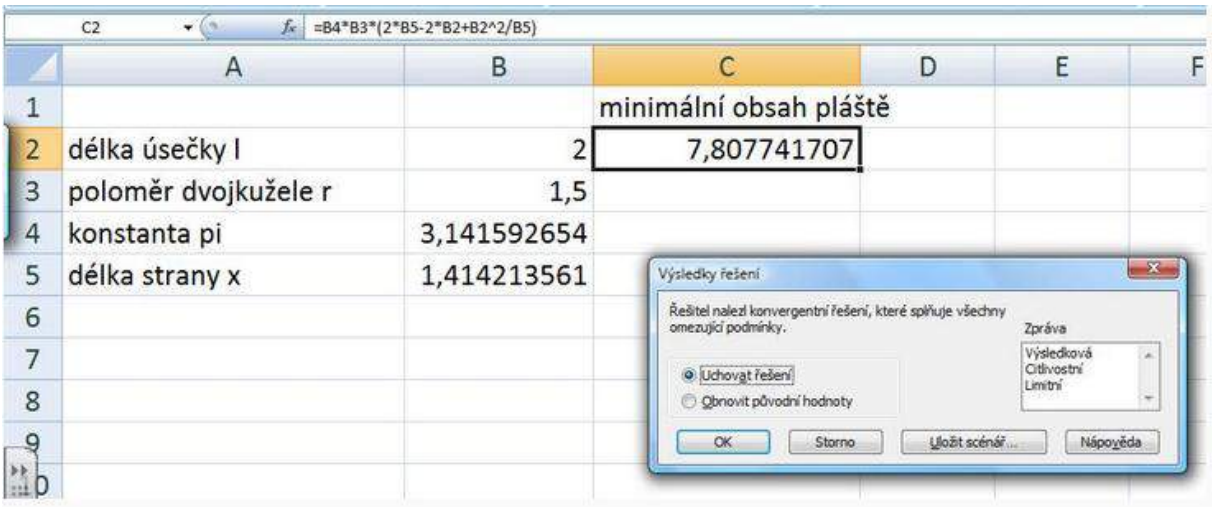

Obr. 5 - vytvořeno pomocí programu MS Excel, Zdroj: vlastní tvorba

Nyní volbou Data -> Řešitel nastavme buňku obsahující délku strany x jako měněnou, buňku se vzorcem pro výpočet obsahu pláště jako buňku s požadovaným minimem v závislosti na x a rovněž zadejme další omezující podmínky podle obrázku.




Obr. 6 - vytvořeno pomocí programu MS Excel, Zdroj: vlastní tvorba

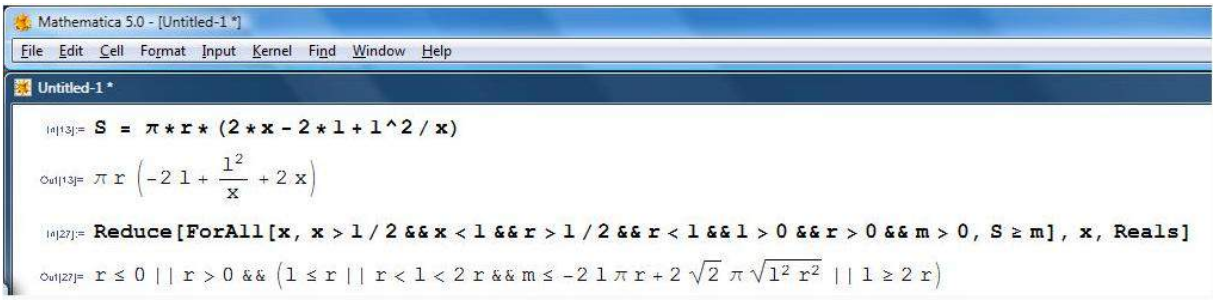
Volbou "Řešit" spustíme řešení, které dává minimální hodnotu obsahu pláště při délce strany x = 1,4142..., viz obrázek.




Obr. 7 - vytvořeno pomocí programu MS Excel, Zdroj: vlastní tvorba

Při pevně dané délce rotující úsečky a vzdálenosti, kterou má od ní mít právě jeden bod úsečky, dosáhneme minimálního obsahu pláště dvojkuželu, pokud bude délka strany většího kužele přibližně 1,414. To je v souladu s výsledky zjištěnými dříve, neboť x:l je v tomto případě také √2:2, tj. 1:√2. Excel vypočte minimální hodnotu obsahu pláště pro nalezené x a pevně zvolené hodnoty. Chceme-li výsledek ve tvaru předpisu s proměnnými l a r, dosadíme ve vztahu $S_{pl} = \pi r[2x - 2l + l^2/x]$ za x hodnotu √2.

B. Máme-li k dispozici program Mathematica aspoň verze 5.0 lze úlohu vyřešit s použitím funkce Reduce, viz obrázek, nebo užitím diferenciálního počtu pomocí funkce D pro derivování a funkce Solve pro řešení rovnic, viz další obrázek.




Obr. 8 - vytvořeno pomocí programu Mathematica, Zdroj: vlastní tvorba

Zadáme předpis pro výpočet obsahu pláště dvojkužele, z nějž chceme vyloučit x za podmínky, aby S bylo minimální. Do funkce Reduce zadáme kvantifikovanou formuli s omezujícími podmínkami. Ve výsledku se orientujeme pomocí znaku ||, které znamená logické "nebo", a znaku &&, který představuje "a zároveň". Na posledním řádku čteme, že minimum m je menší nebo stejné jako hodnota výrazu $-2l\pi r + 2\sqrt{2}\pi\sqrt{(l^2r^2)}$, který lze vzhledem k $\sqrt{(l^2r^2)} = lr$ pro kladná l, r upravit na $2l\pi r(-1 + \sqrt{2})$, když $r < l < 2r$, tj. za podmínek daných úlohou je minimální obsah pláště dán předpisem zjištěným již v (1), (2), (3).

Řešení s využitím diferenciálního počtu v programu Mathematica je zřejmé z dalšího obrázku.

In[35]:= `Solve[D[S, x] == 0]`

Out[35]= $\{\{l \to -\sqrt{2}\, x\}, \{l \to \sqrt{2}\, x\}, \{r \to 0\}\}$

In[36]:= `D[D[S, x], x]`

Out[36]= $\frac{2\, l^2\, \pi\, r}{x^3}$

In[37]:= `% /. x -> l / Sqrt[2]`

Out[37]= $\frac{4\sqrt{2}\, \pi\, r}{l}$

In[38]:= `S /. x → l / Sqrt[2]`

Out[38]= $\left(-2\, l + 2\sqrt{2}\, l\right) \pi\, r$

In[39]:= `Factor[%]`

Out[39]= $2\left(-1 + \sqrt{2}\right) l\, \pi\, r$

Závěrem poznamenejme, že je zajímavým cvičením promyslet, jak se změní uspořádání těles (i jiných útvarů) podle obsahu pláště, když připustíme jiné vztahy mezi r a l a nebudeme trvat na podmínce, že aspoň jeden z krajních bodů úsečky AB je vzdálen právě r.

**Použitá literatura:**


[1] http://www.cut-the-knot.org/do_you_know/isoperimetric.shtml
[2] http://en.wikipedia.org/wiki/Isoperimetric_inequality
[3] Kowal, S., Matematika pro volné chvíle. SNTL: Praha, 1975

**Metodický list pro badatelskou aktivitu 2**

| | | |
|---|---|---|
| Téma | Jednoduché izoperimetrické úlohy | |
| Tematický celek | Extrémy funkcí | |
| Počet žáků | 20 | |
| Věk žáků | 17+ | |
| Pomůcky | Řetízek nebo snadno ohybatelný drátek, případně provázek, čtvercové sítě | |
| Vhodné místo | Běžná či počítačová učebna | |
| Cíle aktivity | Studenti si uvědomí proměnlivost obsahu útvaru při daném obvodu. Budou schopni lépe odhadnout, který ze dvou daných útvarů má větší obsah, resp. menší obvod. Seznámí se s využitím nerovnosti mezi aritmetickým a geometrickým průměrem pro určení extrému funkce. Elementárními postupy budou v jednoduchých případech schopni určit minimální plochu, resp. maximální objem prostorového útvaru. | |
| Rozvíjené kompetence | Kompetence k řešení problémů, kompetence sociální, pracovní, komunikativní | |
| Předchozí znalosti | Výpočet obsahu a obvodu rovinných útvarů, výpočet povrchu a objemu základních prostorových útvarů, řešení rovnic a nerovnic. | |
| Mezipředmětové vztahy | Fyzika, geometrie | |
| Časový plán | Fáze činnosti | Metody a formy, motivace |
| 0-10 | Hledání trojúhelníku daného obvodu s největším obsahem | experimentální činost |

| | | |
|---|---|---|
| 10-15 | Stanovení hypotézy o rovinném útvaru daného obvodu a největšího obsahu | m. dialogu, zobecňování výsledků |
| 15-20 | Úloha o rovinném útvaru s daným obsahem a nejmenším obvodem jako ekvivalentní úloha s předchozí, analogické úlohy v prostoru | užití analogie |
| 20-30 | Zjišťování maximálního objemu tělesa při daných podmínkách | procvičení známých postupů, hledání alternativních metod řešení úlohy |
| 30-40 | Hledání minimálního povrchu tělesa při daných podmínkách | řešení úlohy s využitím počítače |
| 40-45 | Shrnutí výsledků, zhodnocení | |
| Hodnocení | Slovni hodnocení a sebehodnocení v průběhu aktivity | |
| Návaznosti | Infinitesimální počet, variační počet | |

**Multimédia k badatelské aktivitě 2**

**Doporučený multimediální materiál**

Odkazy do internetu k pracovním listům, prezentacím, videím, animacím, apletům nebo jiným dostupným materiálům relevantním k námětu aktivity.

- http://www.cut-the-knot.org/do_you_know/isoperimetric.shtml
- http://en.wikipedia.org/wiki/Isoperimetric_inequality

**Metoda Monte-Carlo**

Jedním z nejstarších popsaných případů využití metody Monte Carlo je problém Buffovy jehly, nazývaný po matematikovi Buffonovi. Ten se roku 1777 snažil dosáhnout hodnoty π náhodným vrháním jehly na linkovaný papír.

Pravděpodobnost, že jehla stejné délky, jako je mezi linkami, po dopadu na papír leží tak, že

protíná některou z linek, je rovna:

Metoda Monte Carlo má dnes již padesátiletou historii. Přesněji byla zformulována a především využívána během druhé světové války. Vymysleli ji vědci Johan von Neumann a Stanislav Ulam ze Spojených států amerických. Přišli na ni při výzkumu chování neutronů a možnosti jejich pronikání různými látkami. Objevil se zde ale problém, a to jak určit procento neutronů v určité sprše, která pronikne například nádrží s vodou. Tento problém nešel řešit ani teoreticky, ani prakticky, i když znali nezbytné údaje. Neumann a Ulam vyřešili problém geniálně, využili k modelování předpovědi známou techniku kola rulety. Odtud také pochází její název Metoda Monte Carlo.

Metoda Monte Carlo je numerická metoda, kterou je možno použít např. pro stanovení odhadu určitých (popř. nevlastních) integrálů, pro nalezení řešení soustav (systémů) rovnic. Kromě toho nachází uplatnění při modelování fyzikálních dějů, zejména v termodynamice. Princip metody spočívá ve formulaci nové úlohy mající náhodný charakter, jejíž řešení se shoduje s řešením původní úlohy, a dále také spočívá v řešení nové úlohy pomocí statistických experimentů. Existují dva možné přístupy při řešení úloh metodou Monte Carlo:

1) geometrická metoda založená na geometrické pravděpodobnosti,

2) výpočet založený na odhadu střední hodnoty náhodné proměnné.

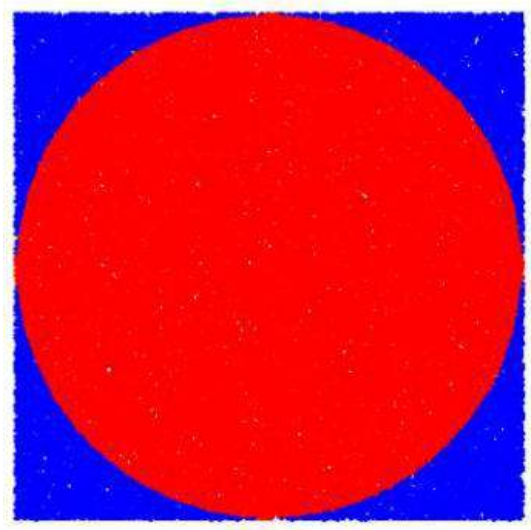
**Motivační příklad - aproximace Ludolfova čísla π**

Velikost obsahu kruhu je dána známým vzorcem $S = \pi r^2$, a tedy čtvrtina velikosti této plochy činí $\frac{\pi r^2}{4}$. Zavedeme souřadný pravoúhlý systém. V prvním kvadrantu zobrazíme jednotkový čtverec, jehož vrchol umístíme do počátku. Nechť tento počátek je středem kruhové výseče, kterou popišme využitím analytické geometrie nerovností $y \leq \sqrt{1-x^2}$. Tuto situaci popisuje obrázek vlevo. Zavedeme sérii náhodných pokusů - vygenerujeme náhodné body $X_i = [x_i, y_i]$, kde $x_i \in \langle 0, 1 \rangle$, $y_i \in \langle 0, 1 \rangle$, $i = 1, 2, \ldots, n$.

Pro názornost je možno tuto sérii spojovat se situací, v níž máme k dispozici *n* herních šipek, které postupně házíme na terč, kterým je onen jednotkový čtverec. Lze očekávat, že některé šipky dopadnou do kruhové výseče, jiné nikoliv. Předpokládejme, že jsme všech *n* šipek vhodili na čtverec. Definujme jev *A* náhodně vybraným bodem ležícím v kruhové výseči.

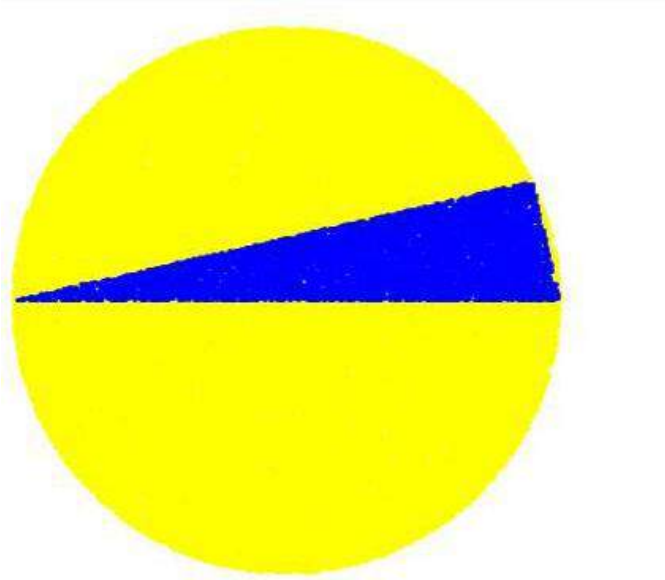
Podle definice geometrické pravděpodobnosti můžeme psát $P(\mathrm{A}) = \frac{\pi r^2 / 4}{r^2} = \frac{\pi}{4}$ Vzdálenost bodu Xi ležícího v kruhové výseči od počátku souřadného systému je dána velikostí radiusvektoru $r = \sqrt{(x_i - 0)^2 + (y_i - 0)^2} = \sqrt{x_i^2 + y_i^2}$ A proto úspěšný pokus nastane, je-li splněna podmínka $\sqrt{x_i^2 + y_i^2} \leq 1$. V opačném případě, tj. pokud bod Xi splňuje podmínku $\sqrt{x_i^2 + y_i^2} > 1$, nastane pokus neúspěšný. Pokud tedy nastane v *n* pokusech *m* úspěšných pokusů, kde $m \leq n$, můžeme psát $P(\mathrm{A}) \approx \frac{m}{n}$. Dále s využitím rovnosti $P(\mathrm{A}) = \frac{\pi r^2 / 4}{r^2} = \frac{\pi}{4}$ je nakonec možno zapsat vztah $\frac{\pi}{4} \approx \frac{m}{n}$ a odtud $\pi \approx \frac{4m}{n}$. Nyní je vše připraveno k implementaci v programu ® Wolfram Mathematica 8 .

Po provedení příkazů uvedených v souborech obsah kruhu a obsah trojúhelníku. Výsledek je zobrazen dále v následujících obrázcích: Rozmístění bodů v kruhu a mimo něj (celkově 100 000 pokusů)



Monte-Carlo aproximace čísla π : 3.14132

Rozmístění bodů v kruhu a mimo něj (celkově 100 000 pokusů)



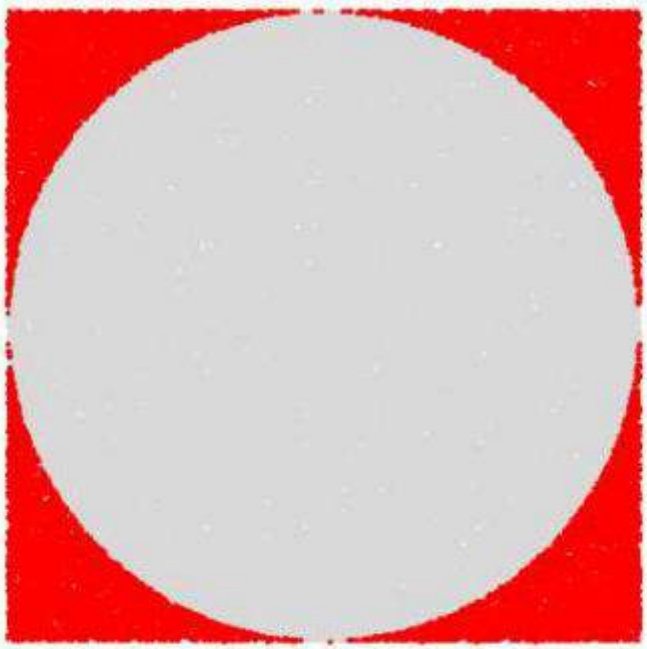
```
Monte-Carlo aproximace obsahu trojúhelníku : 0.43872

Výpočet pomocívzorce : 1/2*v*z = 0.43589
```

První položku (obsah kruhu) můžeme popsat přesněji pomocí metod programu Mathematica (podobně, ale komplikovaněji bychom mohli postupovat v prostředí MS Excel). V následujícím je tento postup popsán.

```
n = 100000;
x0 = 0.9;
data = Table[{RandomReal[{-1, 1}], RandomReal[{-1, 1}]}, {i, 1, n}];
uvnitr = Select[data, #[[1]]^2 + #[[2]]^2 ≤ 1 &];
vne = Select[data, #[[1]]^2 + #[[2]]^2 > 1 &];

Graphics[{LightGray, Point[uvnitr], Red, Point[vne]}]
"Celkový počet bodů je roven " <> ToString[n]
"Počet bodů uvnitř útvaru " <> ToString[Length[uvnitr]]
"Monte-Carlo aproximace obsahu kruhu a zároveň čísla π: " <>
 ToString[N[4 * Length[uvnitr] / n]]
"Skutečná hodnota čísla π = " <> ToString[N[π, 6]]
```



```
Celkový počet bodů je roven 100000

Počet bodů uvnitř útvaru 78334

Monte-Carlo aproximace obsahu kruhu a zároveň čísla π: 3.13336

Skutečná hodnota čísla π = 3.14159
```

Samozřejmě, že můžeme podobný experiment provést i pomocí jednoduchých prostředků – je možné ho provádět pomocí hodů dvou kostek.

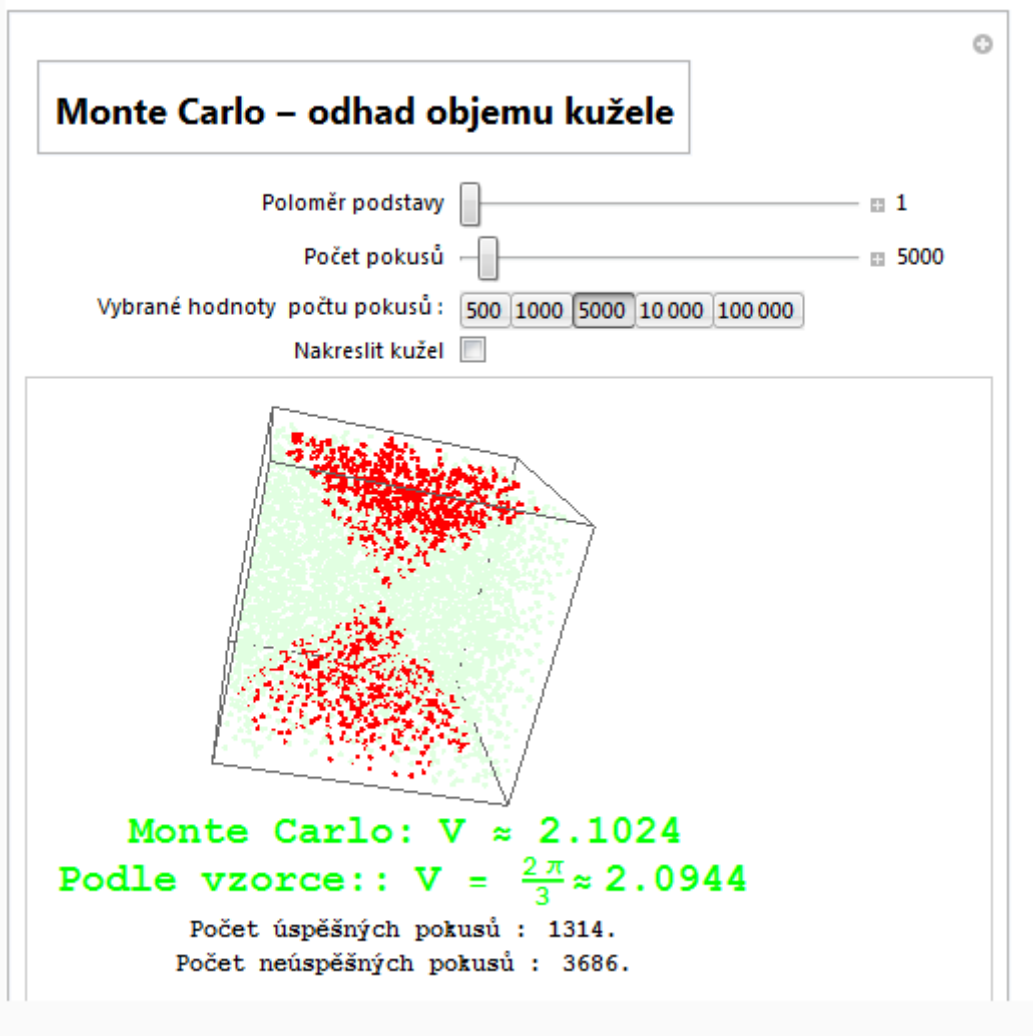
Informace ke stažení ve formátu pdf zde (viz. on-line kurz)

### Praktické ukázky metody

V této kapitole se budeme zabývat skutečnými možnostmi metody a pomocí ní řešit konkrétní úlohy.

První úloha je zjištění objemu kužele (následuje výpis souboru z prostředí Mathematica):

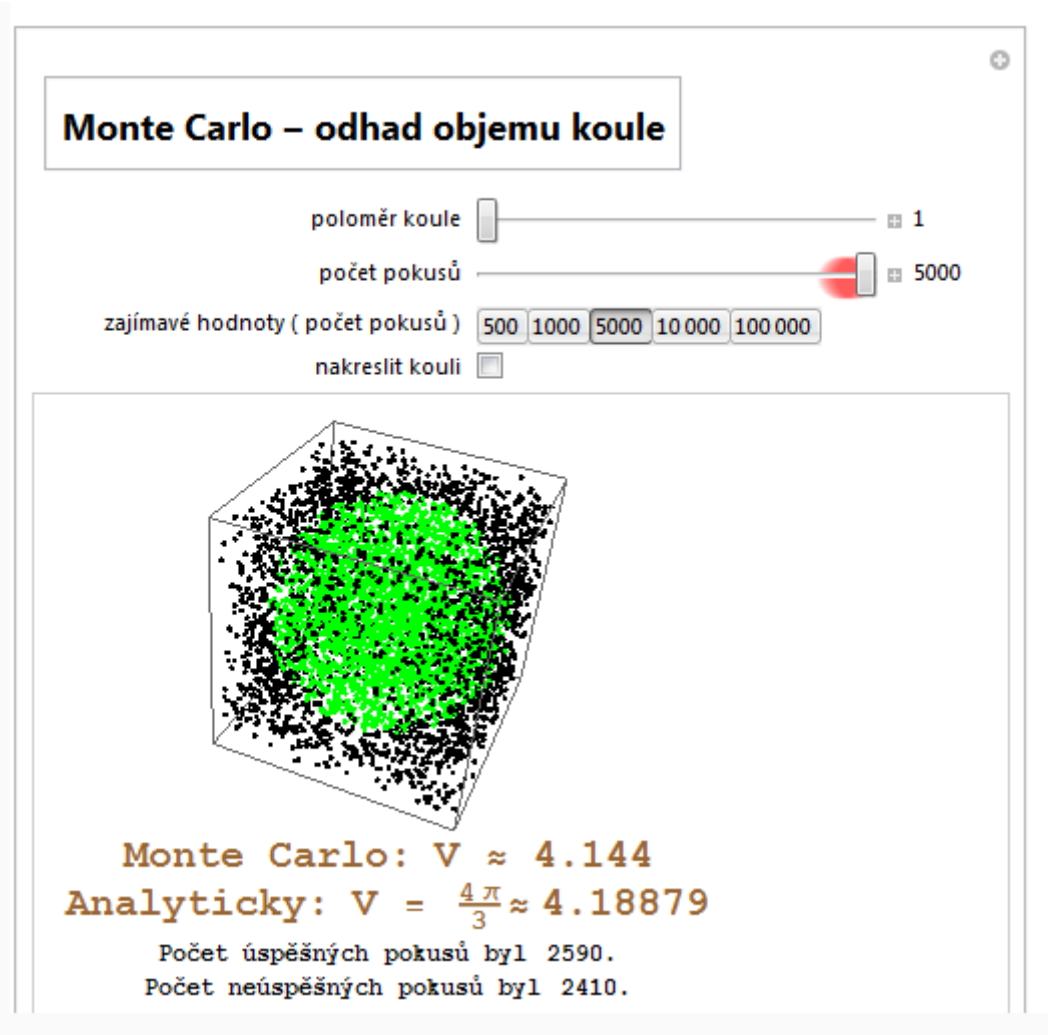
```
Manipulate[If[r > 0 && IntegerQ[pocet] && pocet > 0, {seznam = RandomReal[{-r, r}, {pocet, 3}];
    uspech = Select[seznam, Sqrt[(#[[1]])^2 + (#[[2]])^2] ≤ Abs[(#[[3]])] &];
    neuspech = Select[seznam, Sqrt[(#[[1]])^2 + (#[[2]])^2] > Abs[(#[[3]])] &];
    Column[{Graphics3D[{Red, Point[uspech], LightGreen, Point[neuspech], Opacity[0.3], Pink,
        If[t, Cone[{{0, 0, r}, {0, 0, 0}}, r]]}],
      Style[Row[{"Monte Carlo:", Spacer[10], "V ≈ ", N[8 * r^3 * Length[uspech] / (Length[uspech] + Length[neuspech])]}], Green, Bold, 20],
      Style[Row[{"Podle vzorce::", Spacer[10], "V = ", 2 * Pi * r^3 / 3, "≈", Spacer[5], N[2 * Pi * r^3 / 3]}],
       Green, Bold, 20], Style[Row[{"Počet úspěšných pokusů :", Spacer[10], Length[uspech], "."}], Bold, 12],
      Style[Row[{"Počet neúspěšných pokusů :", Spacer[10], Length[neuspech], "."}], Bold, 12]}, Center]},
   Style["Byly zadány nesprávné parametry.", Red, 14]] // TableForm,
 Panel[Style["Monte Carlo - odhad objemu kužele", 18, Bold]], Row[{}],
 {{r, 1, "Poloměr podstavy"}, 1, 10, 1, Appearance → "Labeled"},
 Control[{{pocet, 5000, "Počet pokusů"}, 1, 100000, 1, Appearance → "Labeled"}],
 Control[{{pocet, 5000, Row[{Spacer[30], "Vybrané hodnoty  počtu pokusů :"}]}, {500, 1000, 5000, 10000, 100000}}],
 {{t, False, "Nakreslit kužel"}, {True, False}}]
```




Je zřejmé, že aproximace objemu je velmi pěkná.

Další praktickou ukázkou je zjištění objemu koule.

```
Manipulate[If[r > 0 && IntegerQ[pocet] && pocet > 0, {seznam = RandomReal[{-r, r}, {pocet, 3}];
    uspech = Select[seznam, Sqrt[(#[[1]])^2 + (#[[2]])^2 + (#[[3]])^2] ≤ r &];
    neuspech = Select[seznam, Sqrt[(#[[1]])^2 + (#[[2]])^2 + (#[[3]])^2] > r &];
    Column[{Graphics3D[{Green, Point[uspech], Black, Point[neuspech], Opacity[0.3], Lighter[Blue],
        If[t, Sphere[{0, 0, 0}, r]]}],
      Style[Row[{"Monte Carlo:", Spacer[10], "V ≈ ", N[8 * r^3 * Length[uspech] / (Length[uspech] + Length[neuspech])]}], Brown, Bold, 20],
      Style[Row[{"Analyticky:", Spacer[10], "V = ", 4 * Pi * r^3 / 3, "≈", Spacer[5], N[4 * Pi * r^3 / 3]}],
       Brown, Bold, 20], Style[Row[{"Počet úspěšných pokusů byl", Spacer[10], Length[uspech], "."}], Bold, 12],
      Style[Row[{"Počet neúspěšných pokusů byl", Spacer[10], Length[neuspech], "."}], Bold, 12]}, Center]},
   Style["Byly zadány nesprávné parametry.", Red, 14]] // TableForm,
Panel[Style["Monte Carlo - odhad objemu koule", 18, Bold]], Row[{}],
{{r, 1, "poloměr koule"}, 1, 10, 1, Appearance → "Labeled"},
Control[{{pocet, 5000, "počet pokusů"}, 1, 100, 1, Appearance → "Labeled"}],
Control[{{pocet, 50000, Row[{Spacer[30], "zajímavé hodnoty ( počet pokusů )"}]}},
  {500, 1000, 5000, 10000, 100000}], {{t, False, "nakreslit kouli"}, {True, False}}]
```




I v tomto případě je aproximace (přibližná hodnota) velmi přesná.

Samozřejmě, že v praktických cvičeních je možné využívat i jiné prostředky - nejjednodušší postup je pomocí dvou či čtyř kostek simulovat hody do rozsáhlého rastru, který je překryt

přes obrázek. Zjistit počet bodů uvnitř obrázku a poté pomocí poměru počtu bodů uvnitř útvaru a celkového počtu bodů nalézt i neznámou plochu či objem.

**Pollardova rho metoda**

Nevýhodou metody opakovaného dělení je její velká výpočtová složitost, pokud bude *n* veliké.

Je tedy přirozené, že se objevovaly alternativní metody. Jednou z nich je Pollardova rho metoda. Byla navržena v r. 1975 a je efektivnější než metoda opakovaného dělení. Poskytuje rovněž náměty k jednoduchému programování.

**Pollardova rho metoda pro faktorizaci přirozených čísel**

V jistém slova smyslu "si hrajeme" s pseudonáhodnými čísly. Zatímco v běžné loterii asi spíše či skoro určitě prohrajeme, v popisované metodě je náhoda naším spoluhráčem a můžeme se dostat rychle k výsledku.

Matematici hrají fair!

1>„Školní“ metoda pro nalezení rozkladu přirozeného čísla N  1 vyžaduje opakovat dělení čísly 2, 3, 4, 5, ... až do té doby, kdy nalezneme číslo dělící N. Pokud však žádné přirozené číslo x $1 < x \leq \sqrt{N}$ „Školní“ metoda pro nalezení rozkladu přirozeného čísla N  , nedělí N, pak je N prvočíslem. V tomto smyslu dává metoda opakovaného dělení vždy výsledek: buďto nalezne netriviální dělitel přirozeného čísla N, nebo poskytne důkaz, že N je prvočíslem. Je ale známo, že metoda opakovaného dělení je velice pomalá. Pro velká N není možné ji nechat v úplnosti proběhnout. Význam této metody pro faktorizaci velkých přirozených čísel je v tom, že ji lze užít jako **první krok** při faktorizaci, přičemž má odhalit **malé** prvočíselné faktory. (Lze vyslovit námitku, že efektivnost této metody by se zlepšila, kdybychom testovali jen dělitelnost prvočísly. To se ale opírá o fakt, že při školních výpočtech máme několik „malých“ prvočísel v paměti a stejně je tomu i při výpočtech počítačových). Závěr, že metoda opakovaného dělení je příliš pomalá, se nemění. Ještě horší je to, jak již víme, v obecném případě s efektivitou Fermatovy faktorizační metody.

, je jednoduchá, elegantní a poskytne nám příležitost seznámit se s některými možnostmi grafických kalkulátorů. Snad tento text poskytne řadu návodů k experimentům, podnětů k napsání jednoduchých matematických programů atd.–Nepřekvapuje proto, že v posledních třiceti letech byly navrženy efektivnější faktorizační algoritmy. Patří mezi ně i faktorizační metoda, navržená J. M. Pollardem v r. 1975. Je vhodné se s touto metodou seznámit

Pollardova rho metoda má pravděpodobnostní charakter. Je v ní zapotřebí nalézt dvě pseudonáhodná čísla $x_n$, $x_m$, mající jistou vlastnost. Následující klasický příklad z teorie pravděpodobnosti dává naději, že na tato „vhodná“ čísla nebudeme čekat dlouho.

**I. Příklad 1:**

Sešla se skupina *n* osob, n je větší nebo rovno 2. Vypočtěte pravděpodobnost, že alespoň dva z nich budou mít narozeniny stejný den v roce. (Pro jednoduchost předpokládejme, že rok má 365 dní, tj. nebereme v úvahu přestupné roky).

**Řešení:**

Určeme pravděpodobnost komplementárního jevu A, že žádné dvě osoby z *n* zúčastněných nebudou mít narozeniny týž den v roce.

Spočtěme nejprve, kolik je všech možných případů pro data narození těchto *n* osob. Pro den narození první osoby je 365 možností, pro dvě osoby je tedy $365^2$ možností, pro *n* osob $365^n$ možností.

Vypočtěme dále, kolik z těchto případů je příznivých. První osoba se může narodit kterýkoli den v roce. Je-li ale již známo její datum narození a nemá -li druhá osoba mít narozeniny týž den, „zbývá“ pro její datum narození již jen 365 - 1 = 364 možností. Nemá-li datum narození žádných dvou osob z n zúčastněných připadnout na stejný den v roce, je 365.364. ... .(365 - *n* + 1) příznivých případů. Proto

$$P(A) = \frac{365.(365-1).(365-2)\ldots(365-k+1)}{365^k}$$

(1) je pravděpodobnost jevu, že žádné dvě osoby z n zúčastněných nebudou mít narozeniny týž den v roce.

Jak si ale vypočítat a případě i znázornit hodnoty pravděpodobností P(A) z (1) pro různá n?

, nejlépe vybavené typy umožňují provádět i symbolické výpočty, resp. stáhnout si do kalkulátoru i programy z interenetu. Pro lepší představu o možnostech grafických kalkulátorů jsou dále zařazeny obrázky displeje kalkulátoru TI-83 Plus firmy Texas Instruments. Jednotlivé body znázorňují hodnoty posloupnosti (1) pro n = 1, 2, ..., 30.;Bylo by jistě možné využít nějakého počítačového programu, ale příslušný software nebývá právě levný. Jak bylo řečeno výše, v posledních zhruba patnácti letech se zprvu v USA, pak v západní Evropě a nyní již i u nás rozšiřují tzv. grafické kalkulátory, které mají víceřádkový displej a umožňují „načrtnout“ grafy funkcí (posloupností). Tyto kalkulátory bývají programovatelné

Získány byly takto:

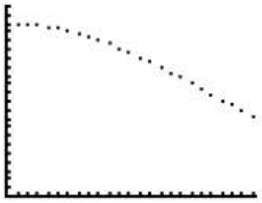
1. V **MODE** nastavme kreslení posloupnosti, tj. **Seq**.

2. V editoru posloupností zadáme u(n) = 365 **nPr** n /365^n, u(nMin) = 1, nMin = 1.

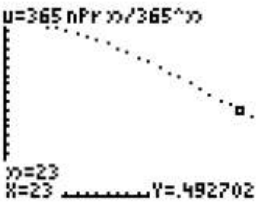
3. Vhodně nastavíme okno (**WINDOW**): nMin = 1, nMax = 30, $X_{min}$ = = -0.1, $X_{max}$ = 28, $X_{scl}$ = 1, $Y_{min}$ = 0, $Y_{max}$ = 1.1, $Y_{scl}$ = 0.05.

4. Po stisku klávesy **GRAPH** dostaneme podle očekávání klesající posloupnost. Viz obr. 1).

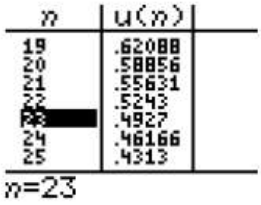
Pomocí povelu **Trace** a kurzorových kláves se lze po těchto bodech pohybovat a odečítat jednotlivé hodnoty. Na obr. 2. je znázorněna hodnota P(A) pro n = 23. Je P(A) = 0,49270277, tj. pravděpodobnost jevu, že mezi 23 osobami nemají žádné dvě narozeniny týž den v roce, je již menší než 50 %. Je tedy „pravděpodobnější", že nastane jev komplementární, tj. že aspoň dva lidé z této skupiny slaví narozeniny týž den v roce. Dále je možné si nechat několik hodnot vypsat do tabulky. Obr. 3 zachycuje displej kalkulátoru, na němž je uvedeno několik hodnot P(A) z (1) pro n = 19, 20, ..., 25.



Obr. 1




Obr. 2




Obr. 3

**II.** Grafické kalkulátory mívají k dispozici povel, kterým jsou generována tzv. pseudonáhodná celá čísla z intervalu $\langle n, m \rangle$, n, m ∈ N, n < m.. Vyzkoušejme povel, který by v závislosti na typu kalkulátoru mohl znít kupř. randInt(n, m) nebo nějak podobně. Kupř. na výše zmíněném kalkulátoru TI-83 Plus se po zadání randInt(1, 6) na displeji objeví jisté přirozené číslo k, pro které $1 \le k \le 6$ čili kalkulačka vlastně simuluje házení kostkou s čísly 1, 2, ..., 6). Obdobně povel randInt(0, 1) poskytuje buď hodnotu 0 nebo 1 a tento výsledek lze interpretovat jako simulaci házení mincí, chápeme-li např. 0 jako líc, 1 - rub. Zmiňme se o metodách pro generování posloupností pseudonáhodných čísel.

Zřejmě nejvíce je využívána tzv. **multiplikativní kongruenční metoda** (multiplicative congruential method), pocházející od D. H. Lehmera (1948). Posloupnosti pseudonáhodných čísel se konstruují tak, že se

1. vypočítají po sobě jdoucí mocniny čísla $a \in N,$

2. získané mocniny se dělí nějakým modulem M, přičemž dostáváme zbytky, které (za určitých předpokladů) tvoří posloupnost pseudonáhodných čísel.

**Pollardova rho metoda II**

**Příklad 2:** Volme a = 4, M = 11.

1. Utvoříme posloupnost několika mocnin $a^k, k \ge 0, k \in Z:$

1, 4, 16, 64, 256, 1024,4096, 16 384, ...

2. Nejmenší nezáporné zbytky při dělení těchto mocnin modulem M = 11 jsou

1, 4, 5, 9, 3, 1, 4, ... .

Samozřejmým cílem studované metody je, aby pokud možno co nejvíce přirozených čísel menších než M bylo členy posloupnosti. Vidíme, že tento cíl se nám nepodařilo splnit a volba a = 4, M = 11 nebyla šťastná. Zvolme proto a = 2, M = 11.

1. Utvořme opět posloupnost několika mocnin $a^k, k \geq 0, k \in Z:$

1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, ...

2. Nejmenší nezáporné zbytky při dělení těchto mocnin modulem M = 11 jsou

1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1, 2, ... .

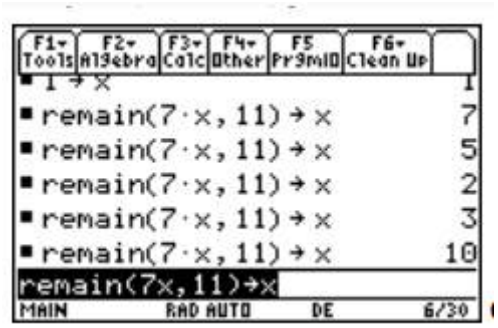
Je jasné, že vytvořená posloupnost musí být periodická, avšak nyní se v získané posloupnosti předtím, než došlo k opakování, objevila všechna přirozená čísla z intervalu 1,10 . (Po sobě jdoucí čísla 1, 2, 4, 8 na začátku této posloupnosti ale nepůsobí „náhodně“).

Volme nyní a = 7, M = 11. Poznamenejme, že některé kalkulátory umožňují přímý výpočet posloupnosti nejmenších nezáporných zbytků při dělení čísel $a^k, k \geq 0, k \in Z:$, modulem M. Kupř. na kalkulátorech TI-89 nebo TI-92 lze zadat

**1 STO → x ENTER**

**remain (7x, 11) STO → x ENTER**

a opakovaně tisknout klávesu ENTER, čímž se realizuje povel zadaný ve druhém řádku. (V prvním kroku se pod hodnotou x uloží (Store) číslo 1, v dalších krocích je vždy počítán zbytek (remainder) při dělení čísla 7x číslem 11).




Tím získáme hledanou posloupnost zbytků 1, 7, 5, 2, 3, 10, 4, 6, 9, 8, 1, ... (viz obr. 4). Kalkulátory TI-83 nemají funkci **remain (m, n)** počítající nejmenší nezáporný zbytek při dělení přirozeného čísla m, číslem $n \in N$, mají však kupř. funkci **iPart(z)**, vracející celou část čísla z, a protože na kalkulátorech této třídy lze vytvářet a ukládat programy, není nijak obtížné funkci **remain(m, n)** naprogramovat (což je užitečným cvičením).

Pokud se týče získané posloupnosti 1, 7, 5, 2, 3, 10, 4, 6, 9, 8, 1, ..., zdá se, že jsme byli úspěšní - získali jsme posloupnost obsahující všechna přirozená čísla z intervalu 1,10 a vypadající „náhodně“. Přistupme proto k zápisu Lehmerovy metody v obecném případě.

- zvolíme číslo M (modul),

- zvolíme násobitel $A \in N$

Posloupnost $\{X_i\}_{i=0}^{\infty}$ vytváříme takto:

$X_1$ je nejmenší nezáporný zbytek při dělení čísla $A.X_0$ číslem M; platí tedy $X_{1=} A.X_0$ (mod M),

$X_2$ je nejmenší nezáporný zbytek při dělení čísla $A.X_1$ číslem M; platí tedy $X_{2=}A.X_1$ (mod M), ...,

$X_{n+1}$ je nejmenší nezáporný zbytek při dělení čísla $A.X_n$ číslem M; platí tedy $X_{n+1} = A.X_n$ (mod M).

V příkladu 2 bylo vždy $X_0 = 1$, M = 11 a násobitel A byl 4, resp. 2, 7.

Jak se uvádí v [2], v praxi se užívá $M = 2^{31} - 1$, $A = 7^5$ a firma IBM užívala podle údajů uvedených v této knize $M = 2^{31}$ a $A = 2^{16} + 3$. Je také samozřejmé, že vygenerované posloupnosti musejí projít řadou statistických testů na náhodnost.

Poznamenejme, že právě popsaná metoda generování pseudonáhodných posloupností přirozených čísel není jediná. Zvolíme-li kupř. jisté přirozené číslo $X_0$ a modul M a položíme - li $X_{i+1} = X_i^2 + 1$ (mod M), i = 0, 1, ..., ukazuje zkušenost, že se často získá posloupnost pseudonáhodných čísel z intervalu $\langle 1, M-1 \rangle$, která je pro užití v Pollardově rho metodě výhodnější než posloupnost generovaná lineární funkcí. Jak se uvádí v [1]: „The choice of this iteration function is black magic, but linear polynomials do not work, and higher degree polynomials are more costly to evaluate, and one cannot prove more about them than about $x^2 + 1$."

Nyní již můžeme přistoupit k formulaci Pollardovy rho metody. Nechť N je přirozené číslo, které chceme faktorizovat. Zvolme přirozené číslo x0 a vypočtěme jistý počet členů posloupnosti nezáporných celých čísel $\{x_i\}$, definovaných následovně:

$x_{i+1} = x_i^2 + 1$ (mod N).

Předpokládejme, že prvočíslo p je nejmenším prvočíselným dělitelem čísla N. Dále předpokládejme, že $\{x_i\}$ je posloupností pseudonáhodných čísel modulo p. Dále, nechť pro jisté dva členy $x_n$, $x_m$, n > m této posloupnosti platí, že $x_n = x_m$ (mod p). (Příklad 1 nám dává naději, že na výskyt takovýchto členů posloupnosti $\{x_i\}$ nebudeme muset čekat dlouho). Platí tedy $p|(x_n - x_m),\ p \mid N$, tedy největší společný dělitel $D(x_n - x_m, N) > 1$. Pokud zároveň $x_n \not\equiv x_m \pmod N,\ \text{je } D(x_n - x_m, N) < N$ a nalezli jsme netriviální vlastní dělitel čísla N. Navíc je výhodné, že tento dělitel lze nalézt Eukleidovým algoritmem, což je, jak víme z druhé části kapitoly 1., velice efektivní metoda.

Krajně neuspokojivé by ale bylo, kdybychom vskutku museli počítat $D(x_n - x_m, N)$ pro všechny dvojice $\text{dvojice } n, m \in N, n > m.$ Objem výpočtů by narostl tak, že by to zcela znehodnotilo praktické využití navrhované metody. Naštěstí lze velkou část těchto propočtů ušetřit. Postačí totiž testovat jen dvojice $x_{2i}, x_i, i \in N$, jak posléze ukážeme. Nyní zapišme nástin algoritmu pro Pollardovu rho - metodu:

Je dáno přirozené číslo N, které chceme rozložit.

1. Zvolme přirozené číslo $x_0$.
2. Vypočtěme $x_{i+1} \equiv x_i^2 + 1 \pmod N$, $i = 0, 1, \ldots$
3. Pro jistý počet $i \in N$ vypočtěme $D(x_{2i} - x_i, N)$.
4. Opakujme to do té doby, než $D(x_{2i} - x_i, N)$ je netriviálním dělitelem čísla N– **úspěch.**

   Pokud proces běží přes daný časový limit – **neúspěch**.

**Pollardova rho metoda III**

**Příklad 3: Rozložme číslo N = 221 pomocí Pollardovy rho - metody**.

Řešení: Volme kupř. $x_0 = 5$ a vypočtěme dalších deset členů posloupnosti $\{x_i\}$. Máme $x_1 = 26$, $x_2 = 14$, $x_3 = 197$, $x_4 = 135$, $x_5 = 104$, $x_6 = 209$, $x_7 = 145$, $x_8 = 31$, $x_9 = 78$, $x_{10} = 118$. Dále

$D(x_2 - x_1, N) = D(14 - 26, 221) = 1,$

$D(x_4 - x_2, N) = D(135 - 14, 221) = 1,$

$D(x_6 - x_3, N) = D(209 - 197, 221) = 1,$

$D(x_8 - x_4, N) = D(31 - 135, 221) = 13.$

Nalezli jsme netriviální dělitel čísla N = 221, je **221 = 13 . 17**.

Vidíme, že výpočet vyžaduje jen provádění elementárních početních operací s celými čísly a výpočet největšího společného dělitele. Bude -li tedy číslo N malé, byl by podobný výpočet dostupný i žákům ZŠ a mohl by možná zaujmout ty z nich, kteří mají hlubší zájem o matematiku.

**Příklad 4: Pomocí Pollardovy rho - metody rozložme číslo N = 989.**

Řešení: Volme kupř. $x_0 = 10$. Je pak $x_1 = 101$, $x_2 = 312$, $x_3 = 423$, $x_4 = 910$, $x_5 = 308$, $x_6 = 910$, $x_7 = 308$, $x_8 = 910$, $x_9 = 308$, $x_{10} = 910$ atd. Dále máme $D(x_2 - x_1, N) = D(312 - 101, 989) = 1$, $D(x_4 - x_2, N) = D(910 - 312, 989) = 23$.

Nyní snadno nalezneme rozklad **N = 989 = 23.43.** Měli jsme štěstí, rozklad čísla N byl nalezen rychle.

Je však zapotřebí uvést, že Pollardova ρ – metoda může také selhat. Může se to stát v případě, že pro nejmenší číslo i takové, že $D(x_{2i} - x_i, N) > 1$, je $x_{2i} - x_i$ násobkem čísla N. V [2] se uvádí příklad N = 1241, $x_0 = 6$: pak je $x_1 = 37$, $x_2 = 129$, $x_3 = 509$, $x_4 = 954$, $x_5 = 464$, $x_6 = 604$, $x_7 = 1204$, $x_8 = 129$, $x_9 = 509$, $x_{10} = 954$, $x_{11} = 464$, $x_{12} = 604$. Dále obdržíme $D(x_2 - x_1, N) = D(129 - 37, 1\,241) = 1$,

$D(x_4 - x_2, N) = D(954 - 129, 1\,241) = 1$,

$D(x_6 - x_3, N) = D(604 - 509, 1\,241) = 1$,

$D(x_8 - x_4, N) = D(129 - 954, 1\,241) = 1$,

$D(x_{10} - x_5, N) = D(954 - 464, 1\,241) = 1$,

$D(x_{12} - x_6, N) = D(604 - 604, 1\,241) = 1\,241$.

To ovšem neznamená, že Pollardova metoda selhala všeobecně – bylo jen zvoleno „nevhodné“ $x_0$. Vezměme opět N = 1 241 a $x_0 = 7$. Pak je $x_1 = 50$, $x_2 = 19$, $x_3 = 362$, $x_4 = 740$, $x_5 = 320$, $x_6 = 639$, $x_7 = 33$, $x_8 = 1\,090$, $x_9 = 464$, $x_{10} = 604$, $x_{11} = 1204$, $x_{12} = 129$, $x_{13} = 509$, $x_{14} = 954$ atd. Dále

$D(x_2 - x_1, N) = D(19 - 50, 1\,241) = 1$,

$D(x_4 - x_2, N) = D(740 - 19, 1\,241) = 1$,

$D(x_6 - x_3, N) = D(639 - 362, 1\,241) = 1$,

$D(x_8 - x_4, N) = D(1\,090 - 740, 1\,241) = 1$,

$D(x_{10} - x_5, N) = D(604 - 320, 1\,241) = 1$,

$D(x_{12} - x_6, N) = D(129 - 639, 1\,241) = 17$.

Poté již snadno nalezneme rozklad **N = 17. 73**.

**Příklad 5: Pomocí Pollardovy rho - metody rozložme číslo N = 4 004 747.**

**Řešení:** Volme kupř. $x_0 = 100$. Máme $x_1 = 10\ 001$, $x_2 = 3\ 906\ 074$, $x_3 = 820\ 973$, $x_4 = 1\ 751\ 377$, $x_5 = 1\ 569\ 143$, $x_6 = 3\ 194\ 416$, $x_7 = 1\ 992\ 454$, $x_8 = 3\ 283\ 740$, $x_9 = 2\ 895\ 474$, $x_{10} = 39\ 551$. Dále obdržíme

$D(x_2 - x_1, N) = D(3\ 906\ 074 - 10\ 001, 4\ 004\ 747) = 1$,

$D(x_4 - x_2, N) = D(1\ 751\ 377 - 3\ 906\ 074, 4\ 004\ 747) = 163$.

Nalezli jsme netriviální dělitel čísla N. Mohli bychom teď faktorizovat číslo $N' = \frac{N}{163} = 24\ 569$. Druhou možností je pokračovat ve výpočtech. Je dále

$D(x_6 - x_3, N) = D(3\ 194\ 416 - 820\ 973, 4\ 004\ 747) = 163$,

$D(x_8 - x_4, N) = D(3\ 283\ 740 - 1\ 751\ 377, 4\ 004\ 747) = 12\ 877$.

Snadno zjistíme, že $12\ 877 = 79.163$ a rovněž lehce nahlédneme, že **N = 79. 163. 311.**

**Příklad 6: Pomocí Pollardovy rho - metody rozložme číslo N = 63 797.**

**Řešení:** Volme kupř. $x_0 = 25$. Kalkulátory umožňující provádět symbolické výpočty mají též povely pro práci s maticemi, resp. se seznamy prvků (Lists). Není tedy příliš obtížné si vytvořit seznam prvků vhodné délky, obsahující prvky $x_i$, $i \in \{1, 2, ..., s\}$ (na kalkulátorech třídy TI-89 či TI-92 mohou seznamy prvků obsahovat až 999 prvků). Poté je možné napsat program, který by testoval, zda pro jisté $i \in \{1, 2, ..., s\}$ splňuje prvek $d = D(x_{2i} - x_i, N)$ nerovnosti $1 < d < N$. V takovém případě je nalezen netriviální dělitel d čísla N. Celá věc je jednoduchým programátorským cvičením.

V daném případě bychom mohli nejprve utvořit posloupnost, řekněme, prvních třiceti členů posloupnosti $\{x_i\}$, tj. $x_1 = 626$, $x_2 = 9\ 095$, $x_3 = 38\ 114$, $x_4 = 19\ 307$, $x_5 = 58\ 176$, $x_6 = 16\ 127$, $x_7 = 43\ 558$, $x_8 = 40\ 382$, $x_9 = 54\ 605$, $x_{10} = 25\ 637$, $x_{11} = 19\ 076$, $x_{12} = 59\ 486$, $x_{13} = 19\ 795$, $x_{14} = 852$, $x_{15} = 24\ 138$, $x_{16} = 48\ 841$, $x_{17} = 9\ 655$, $x_{18} = 11\ 609$, $x_{19} = 29\ 618$, $x_{20} = 17\ 175$, $x_{21} = 47\ 095$, $x_{22} = 36\ 321$, $x_{23} = 20\ 676$, $x_{24} = 57\ 077$, $x_{25} = 53\ 922$, $x_{26} = 33\ 810$, $x_{27} = 1\ 455$, $x_{28} = 11\ 725$, $x_{29} = 56\ 888$, $x_{30} = 14\ 126$.

Dále zjistíme, že $D(x_2 - x_1, N) = 1$, $D(x_4 - x_2, N) = 1$, $D(x_6 - x_3, N) = 1$, $D(x_8 - x_4, N) = 1$, $D(x_{10} - x_5, N) = 1$, $D(x_{12} - x_6, N) = 1$, $D(x_{14} - x_7, N) = 131$. Zjišťujeme, že číslo N je součinem dvou prvočísel, **N = 131.487.**

Abychom nahlédli, proč se v názvu studované metody objevilo řecké písmeno ρ, vypočtěme ještě nejmenší nezáporné zbytky $r_i$ při dělení čísel $x_i$ číslem $p = 131$, tj. $x_i \equiv r_i \pmod{131}$, $i = 0, ..., 30$. Je $r_0 = 25$, $r_1 = 102$, $r_1 = 56$, $r_3 = 124$, $r_4 = 50$, $r_5 = 12$, $r_6 = 14$, $r_7 = 66$, $r_8 = 34$, $r_9 = 109$, $r_{10} = 92$, $r_{11} = 81$, $r_{12} = 12$, $r_{13} = 14$, $r_{14} = 66$, $r_{15} = 34$, $r_{16} = 109$, $r_{17} = 92$, $r_{18} = 81$, $r_{19} = 12$ atd. Vidíme, že se v posloupnosti $\{r_i\}$ vyskytuje cyklus délky 7, začínající číslem 12. Znázorníme -li celou situaci uzlovým diagramem, získáme něco, co se podobá písmenu ρ:

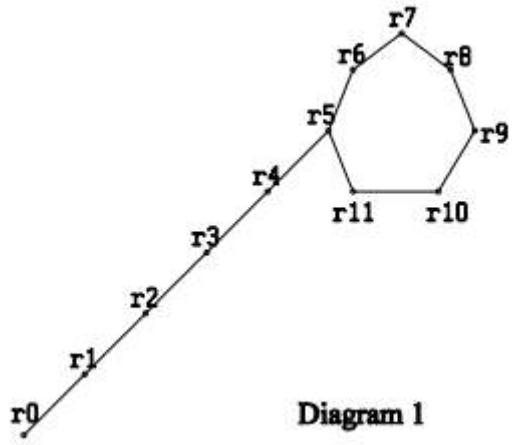



**Diagram 1**

Obecně je jasné, že posloupnost $\{r_i\}_{i=1}^{\infty}$, tvořená jen čísly z množiny $\{0, 1, ..., p - 1\}$ a definovaná rekurentně, se bude opakovat. Kupř. na diagramu 1 vidíme, že po „předperiodě" délky $u = 5$ dochází k probíhání cyklu délky $v = 7$. Jak obdobné cykly efektivně nalézt?

Zatím jsme postupovali poněkud naivně. Vytvořili jsme seznam prvků různé délky a poté máme možnost utvořený seznam procházet a zjišťovat, zda se nějaká hodnota nevyskytne podruhé. V paměti kalkulátoru (počítače) ale musíme mít uloženo $u + v$ prvků seznamu, kde u je délka předperiody a v délka cyklu. Seznamme se ještě s Floydovým trikem pro hledání cyklů, jehož výhodou je, že využívá jen omezený (a pevný) rozsah paměti. Zde je hlavní ideou to, že se kromě posloupnosti $\{r_i\}_{i\in N}$ vytváří ještě posloupnost $\{y_i\}_{i\in N}$, kde $y_i = r_{2i}$ pro všechna $i \in N$. „Rychlejší" posloupnost $\{y_i\}_{i\in N}$ „dožene" pomalejší $\{r_i\}_{i\in N}$ pro jisté $i \in N$, tj. platí pak $r_i = y_i = r_{2i}$.

Sledujme vše na diagramu 1. Vyjde $r_7 = y_7 = r_{14}$. Teď již je jasné, proč v Pollardově algoritmu počítáme jen $D(x_{2i} - x_i, N)$ a ne $D(x_n - x_m, N)$ pro všechna $m, n \in N, n > m$.

**Cvičení: Dokažte platnost této věty:**

**Věta:** Nechť p je prvočíslo dělící číslo N a nechť $x_0$ je dané přirozené číslo. Nechť v posloupnosti $\{x_i\}$, kde $x_{i+1} \equiv x_i^2 \pmod p$, $i = 0, 1, \ldots$, existují taková $m, n \in N$, $m < n$, že $x_n \equiv x_m \pmod p$. Potom pro jisté $t \in N$ platí $x_{2t} \equiv x_t \pmod p$.

Návod: Postupujte podle tohoto schématu:

1. Pišme $n = m + d$, $d \geq 1$. Ukažte, že $x_{m+1} \equiv x_{m+d+1} \pmod p$ a dále indukcí, že $x_{m+r} \equiv x_{m+d+r} \pmod p$ pro všechna $r \in N$.

2. Mezi čísly $m, m + 1, \ldots, m + d - 1$ je právě jedno násobkem čísla d. Předpokládejme, že k je ten index z množiny $\{0, 1, \ldots, d-1\}$, pro který $d \mid m + k$. Potom $m + k = d$ . e pro jisté $e \in N$, $x_{ed} \equiv x_{m+k} \equiv x_{m+k+d} \equiv x_{ed+d} \pmod p$.

3. Dokažte, že obdobně platí $x_{ed} \equiv x_{ed+2d} \pmod p$, $x_{ed} \equiv x_{ed+3d} \pmod p$, ..., $x_{ed} \equiv x_{ed+ed} \equiv x_{2ed} \pmod p$. Položíme -li nyní $t = ed$, máme $x_{2t} \equiv x_t \pmod p$, což bylo dokázati.

Nyní můžeme uvést zápis Pollardovy ρ – metody (upraveno podle [1], zápis v pseudokódu).

**Vstup:** přirozené číslo N, které není ani prvočíslem ani mocninou přirozeného čísla

**Výstup:** buďto vlastní dělitel čísla N, nebo „nezdar“

1. Zvol $x_0 \in \{0, 1, \ldots, N-1\}$ náhodně, $y_0 \leftarrow x_0$, $i \leftarrow 0$

2. **repeat**

3. $i \leftarrow i + 1$, $x_i \leftarrow x_{i-1}^2 + 1$ rem N, $y_i \leftarrow (y_{i-1}^2 + 1)^2 + 1$ rem N

4. $d \leftarrow \gcd(x_i - y_i, N)$

**if** $1 < d < N$ **then return** d

**else if** $d = N$ **then return** „nezdar“

Pro ty, kteří budou chtít naprogramovat kalkulátor podle shora uvedeného návodu, by samozřejmě byla užitečná informace, kolik asi členů posloupnosti $\{x_i\}$ bude nutné vypočítat. Ukazuje se, že pokud N je složené přirozené číslo, p jeho prvočíselný dělitel, pak by měl postačovat výpočet $D(x_{2t} - x_t, N)$ pro $t = 1, 2, \ldots, [2\sqrt{p}]$, „téměř ve všech případech“ (zde $[a]$ značí celou část čísla $a$ a průběh výpočtu ovšem má nám již známý „pravděpodobnostní“ charakter).

Před třiceti lety byla Pollardova rho - metoda jednou z nejúčinnějších faktorizačních metod. V roce 1981 se např. Brentovi a Pollardovi zdařilo pomocí této metody rozložit osmé Fermatovo číslo $F_8 = 2^{2^8} + 1 = p_{16} \cdot p_{62}$, tedy v součin dvou prvočísel majících 16, resp. 62 cifer. Jak je patrné z následující tabulky, dnes již toto postavení ztratila a byla překonána

několika efektivnějšími, ovšem i komplikovanějšími metodami. Pro školskou matematiku však má Pollardova rho - metoda mnohé přednosti - je jednoduchá a přináší mnoho podnětů k samostatné práci žáků, příležitosti k seznámení se s grafickými kalkulátory, resp. se základy programování.

Z knihy [1] je převzata tabulka popisující dobu běhu některých algoritmů užívaných pro faktorizaci přirozeného čísla N délky n na jeho prvočíselné faktory. Doba běhu Lenstrova algoritmu ve skutečnosti nezávisí na n, ale (hlavně) na délce druhého největšího prvočíselného faktoru čísla N. Některé z časových analýz jsou pouze heuristické, ne rigorózně dokázané. Poznamenejme, že velikost vstupu je $n \approx \log_2 N/64$ slov.

| metoda | rok | čas |
|---|---|---|
| opakované dělení | $-\infty$ | $O^{-}(2^{n/2})$ |
| Pollardova $p-1$ metoda | 1974 | $O^{-}(2^{n/4})$ |
| Pollardova $\rho$ – metoda | 1975 | $O^{-}(2^{n/4})$ |
| Pollardova a Strassenova metoda | 1976 | $O^{-}(2^{n/4})$ |
| Morrisonova a Brillhartova metoda řetězových zlomků | 1975 | $\exp O^{-}((n^{1/2}))$ |
| Dixonova metoda náhodných čtverců | 1981 | $\exp O^{-}((n^{1/2}))$ |
| Lenstrova metoda eliptických křivek | 1987 | $\exp O^{-}((n^{1/2}))$ |
| metoda síta v číselných tělesech | 1990 | $\exp O^{-}((n^{1/3}))$ |

**Tab. 1.**

Literatura:

[1] von zur Gathen, J, Gerhard, J.: Modern Computer Algebra, Cambridge University Press, 1999.

[2] Childs, L. N.: A Concrete Introduction to Higher Algebra, Springer, New York, 1979.

[3] Pomerance, C.: Vyprávění o dvou sítech. PMFA, 43 (1998), 9 - 29.

[4] Riesel, H.: Prime Numbers and Computer Methods for Factorization, 2. vydání, Birkhäuser, 1994.

Seznámili jsme se s moderní faktorizační metodou, ale její idea je dostupná i studentu SŠ se zájmem o matematiku.

Informace ke stažení ve formátu pdf zde.

**Matematické rébusy**

Jak jsme popsali v článku Možnosti a typy popularizace matematiky, významným motivačním činitelem v získání zájmu o studium matematiky může být tzv. rekreační matematika. Ta nabízí celou řadu zábavných početních úkolů a logických rébusů, přičemž právě rébusů je dosti velké množství. Podívejme se na několik z nich a naznačme způsoby jejich řešení.

**Úkol 1:** Řešte sudoku.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 5 | | | 9 | 7 | | | | |
| 1 | | | | | | | | 9 |
| 4 | | | | 1 | 3 | 5 | | |
| | | | | 6 | | | | |
| | | 7 | | | | 3 | | |
| 2 | 9 | | | 5 | | | 1 | |
| | | 3 | 2 | | | | | |
| | 4 | 1 | 5 | | | 7 | | |
| 6 | 5 | | | 4 | | 9 | | |

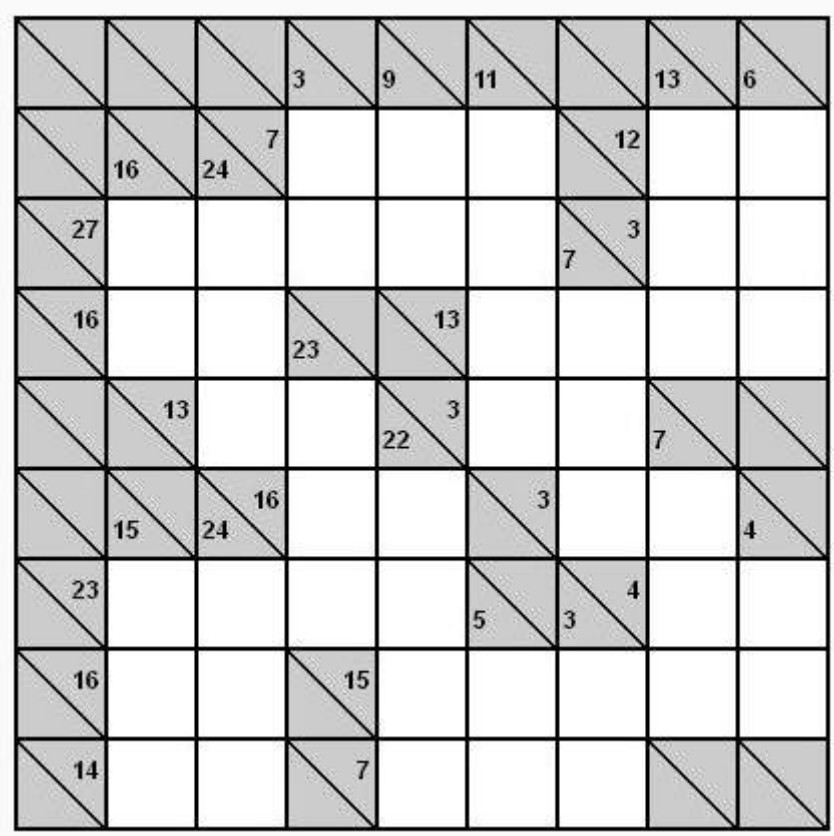
*Zadání sudoku (zdroj: Sudoku Zdarma)*

**K řešení:** Sudoku patří mezi nejznámější matematické rébusy známé téměř v celém světě. Řešitel má zadanou čtvercovou síť 9x9 políček s devíti zvýrazněnými čtverci o délce hrany 3 políčka. V některých z políček jsou již zadána konkrétní čísla od 1 do 9 a řešitelovým úkolem je doplnit do zbývajících prázdných polí čísla tak, aby byla dodržena následující pravidla:

- v každém sloupečku velkého čtverce o hraně 9 políček se vyskytuje každé z čísel 1 až 9 právě jednou,
- v každém řádku velkého čtverce o hraně 9 políček se vyskytuje každé z čísel 1 až 9 právě jednou,
- v každém malém čtverci o hraně 3 políčka se vyskytuje každé z čísel 1 až 9 právě jednou.

Zadání klasických sudoku (i některých jeho dalších variant) je možné najít ve specializovaných knihách či na vybraných webových stránkách nepřeberné množství. Stejně tak existuje velké množství aplikací pro chytré telefony a tablety, které dokážou generovat vlastní originální zadání. Spolu s tím jsou dostupné i on-line nástroje na jejich strojové řešení, které je v případě sudoku relativně jednoduché.

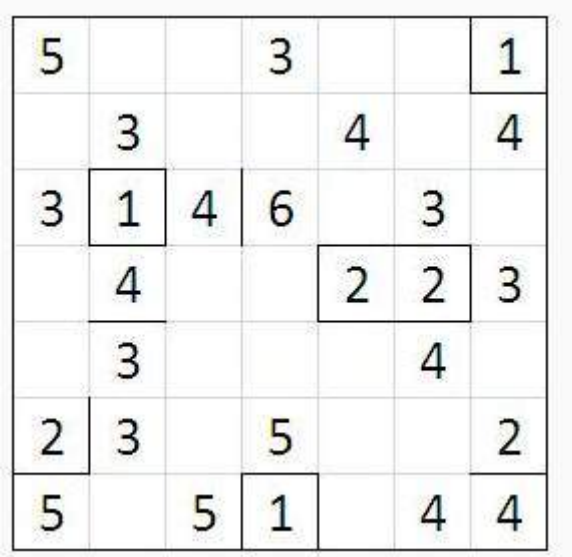
**Úkol 2:** Řešte kakuro.



*Zadání kakura (zdroj: Kakuro Conquest)*

**K řešení:** Kakuro je logický matematický rébus, který na první pohled připomíná křížovku. Na rozdíl od ní se však do jednotlivých políček nevyplňují písmenka, ale čísla, která mohou nabývat hodnot 1 až 9, přičemž jejich součet musí odpovídat číslu vyskytujícímu se v záhlaví části sloupce či řádku, v němž se nalézají. Podobně jako v sudoku platí, že v každé samostatné části sloupce či řádku se žádné z již použitých čísel nesmí opakovat. Rozdíl na druhou stranu spočívá v tom, že hrací síť nemá pevně daný tvar a může být teoreticky libovolně velká.

**Úkol 3:** Řešte fillomino.




*Fillomino se zadanými čísly a s částí vyznačených hranic mezi polyominy (zdroj: Fillomino: Play fillomino online)*

**K řešení:** Třetím zmíněným rébusem je fillomino, které stejně jako kakuro nemá pevně danou velikost ani tvar hrací sítě (tvar však obyčejně bývá obdélníkový). V některých polích jsou již dána čísla, která mohou nabývat hodnot od 1 výše (horní mez v podstatě není pevně daná a v teoretickém případě nekonečně velké hrací sítě by mohla být také nekonečně velká), ostatní pole jsou prázdná. Cílem hry je rozdělit tuto síť do polyomin (monomino zahrnuje 1 políčko, domino zahrnuje 2 sousední políčka, triomino 3 sousední políčka,...) a vyznačit jejich ohraničení tak, že každé z již zadaných čísel *n* bude ležet na polyominu sestávajícím z *n* políček. Jediné pravidlo při řešení spočívá v tom, že žádná dvě stejná polyomina spolu nesmí sousedit a dotýkat se smí maximálně rohy.

**Multimédia k badatelské aktivitě**

Na internetu i v knihách lze dohledat velké množství nejrůznějších zadání zmíněných matematických rébusů. Uveďme zde několik odkazů na webové stránky týkající se sudoku, kakura a fillomina.

Sudoku:

- Sudoku Online
- Sudoku Zdarma

Kakuro:

- Kakuro Online
- Kakuro Conquest

Fillomino:

- Fillomino puzzles
- BrainBashes: Daily Fillomino
- Fillomino Online (Logical Thinking Puzzle Game)

odkazy viz. on-line kurz